الجمـهورية الجزائرية الديمقراطية الشعبيـة
وزارة التعليم العالي والبحث العلمي
جـامعـة سعـيـدة د.مـولاي الطـاهـر
كـليـة التكنولوجيا
قسم: الإعلام الآلي

Mémoire de Master

Spécialité : Sécurité Informatique et Cryptographie

Thème

Méthode hybride pour la détection Et le filtrage de spam image

Présenté par :
TAGUINE ZAKARIA
AGGOUN HADJ ABDERRAHMANE

Dirigé par :
Dr. LATRECHE Abdelkrim

Remerciements

Nous rendons grâce à Dieu qui nous a donné l'aide, la patience, le courage pour accomplir ce travail et nous a maintenu en santé pour mener à bien cette année d'étude.

Nous tenons à adresser nos remerciements à notre encadreur Monsieur le Dr. LATRECHE Abdelkrim qui nous a aidés à élaborer ce projet.

Nos remerciements s'adressent aussi aux Mrs les jurés pour l'intérêt qu'ils ont porté à ce travail en acceptant d'être examinateurs.

Nos remerciements à tous ceux qui nous ont aidé de près ou de loin réaliser ce mémoire surtout Hamou djillali med redha (notre camarade qui nous a aider à élaborer ce travail.

Dédicace

Nous dédions ce mémoire à :

Nos chers parents :

Que nulle dédicace ne puisse exprimer ce que nous leurs devons, pour tous leurs sacrifices leur bienveillance, leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études. Que ce travail soit témoignage de notre profond amour et notre grande reconnaissance « Que Dieu vous garde ».

Nos chères sœurs et nos chers frères :

Pour leurs encouragements permanents, et leur soutien moral, Nous leur dédie ce modeste travail en témoignage de notre grand amour et notre gratitude infinie.

Tous nos amis :

Pour leur aide et leur soutien moral durant l'élaboration du travail de fin d'études.

Table des matières

Remerciements 2

Dédicace 3

Liste des tableaux 7

Liste des équations : 7

Table des sigles et acronymes 8

Introduction Générale 9

Chapitre 1 : Détection et filtrage de spam image 12

1.1 Introduction 13

1.2 Notions sur le spam 13

1.2.1 Définition du spam 13

1.2.2 Types de spam 13

1.2.3 Objectifs des spam 15

1.2.4 Statistiques sur les spam 15

1.2.5 Impactes du spam sur les utilisateurs et les fournisseurs : 17

1.3 Notions sur le spam image 17

1.3.1 Définition 17

1.3.2 Les types 17

1.3.3 Types de spam images 19

1.3.4 Filtrage de spam image : 24

1.3.5 Travaux connexes 25

1.4 Conclusion : 27

Chapitre 2 : Analyse de la Texture 28

2.1 Introduction 29

2.2 Définition de l'image 29

2.3 Typologie d'image 30

2.4 Caractéristiques d'une image numérique 30

2.5 Définition de la texture 33

2.5.1 Types de texture 34

2.6 Analyse visuelle de la texture 36

2.7 Méthodes d'analyse de texture 37

2.8 Notions d'attribut et de descripteur de texture 39

2.9 Conclusion 39
Chapitre 3 : Conception *40*
3.1 Introduction 41
3.2 Architecture générale du système 41
3.2.1 Ensemble de données 42
3.2.2 Prétraitement 42
3.2.3 Extraction des caractéristiques 43
3.2.4 Méthode de la Matrice de cooccurrence des niveaux de gris 43
3.2.5 La méthode des motifs binaires locaux (LBP : local binary pattern) 51
3.2.6 Combinaison des caractéristiques 56
3.2.7 Classification 56
3.3 Conclusion 58
Chapitre 4 : implémentation et expérimentation *60*
4.1 Introduction 61
4.2 Outils d'implémentation 61
4.3 Environnement d'implémentation 62
4.4 Ensemble de données 62
4.5 Implémentation et Réalisation 63
4.5.1 Le module de prétraitement 63
4.5.2 Le module d'extraction des caractéristiques 63
4.5.3 Le module de classification 63
4.6 Résultats obtenus et discussions 63
4.6.1 Dataset1 (dredze) 65
4.6.2 Dataset2 (IHS) 68
4.6.3 Dataset3 (Combine) 70
4.7 L'interface de l'application 74
4.8 Conclusion 76
Conclusion générale *77*
Bibliographie *78*
ملخص *79*
Abstract *79*
Résumé *79*

Table de figure :

Figure 1 : Premier spam sur le réseau ARPANET2, Gary Thuerk. 14
Figure 2:Le volume de spam emails du 4th quart 2016 to 1st quart 2018. 16
Figure 3:Exemples de spam image (Yan Gao et al., 2008). 18
Figure 4:Exemples de spams images (i) financiers, (ii) produits, (iii) Internet et (iv) loisirs 19
Figure 5:Exemple d'image non spam de l'ensemble de données 19
Figure 6:Spam image texte uniquement 20
Figure 7:Image avec pixel de couleur aléatoire 20
Figure 8:Exemples d'obscurcissement utilisés dans le spam d'image. 21
Figure 9:Image découpé 21
Figure 10:Image avec fond sauvage. 22
Figure 11:Exemple de spam image Gifs animés multi-images. 22
Figure 12:Exemple de spam image de dessin animé. 23
Figure 13:Exemple de spam images naturelles / standards. 24
Figure 14:exemple d'image 30
Figure 15:Groupe de pixel 31
Figure 16:(a) Image sans bruit. (b) Image avec bruit 31
Figure 17:Contour d'une image. 32
Figure 18:Image avec histogramme. 33
Figure 19:Exemples de textures ordonnées 34
Figure 20:Exemples de textures aléatoires 35
Figure 21:Exemples de textures hybrides 35
Figure 22:Base d'images de texture de Brodatz 35
Figure 23:Primitive et échelle d'observation 36
Figure 24 : Architecture générale 41
Figure 25:Exemples des directions de la matrice de cooccurrence 45
Figure 26:Opérateur LBP. 51
Figure 27:Exemples de voisinages utilisés pour le calcul des LBP. 51
Figure 28:Primitives extraites par les motifs binaires locaux. 52
Figure 29:: Trois voisinages pour des R et P différents, (b) : Textures particulières détectées par $LBPu2$. 53
Figure 30:Motifs binaires locaux uniformes 2 et invariants en rotation. 53
Figure 31:Les 36 modèles binaires uniques invariants en rotation qui peuvent apparaître 54
Figure 32:Exemple d'un histogramme LBP d'une image faciale. 55
Figure 33:K voisins les plus proches 57
Figure 34:Machines à support vectoriels (SVM) 58
Figure 35:matrice de confusion (GLCM + SVM) 66
Figure 36:matrice de confusion (LBP + SVM) 66
Figure 37:matrice de confusion (GLCM-LBP + SVM) 66
Figure 38:Courbe ROC (GLCM + SVM) 67
Figure 39:Courbe ROC (LBP + SVM) 67
Figure 40:Courbe ROC (GLCM-LBP + SVM) 67

Figure 41:matrice de confusion (GLCM + SVM) 68
Figure 42:matrice de confusion (LBP + SVM) 68
Figure 43:matrice de confusion (GLCM-LBP + SVM) 69
Figure 44:courbe ROC (GLCM+SVM) 69
Figure 45: Courbe ROC (LBP + SVM) 69
Figure 46:Courbe ROC (GLCM-LBP + SVM) 70
Figure 47:matrice de confusion (GLCM + SVM) 71
Figure 48:matrice de confusion (LBP + SVM) 71
Figure 49:matrice de confusion (GLCM-LBP + SVM) 71
Figure 50:Courbe ROC (GLCM + SVM) 72
Figure 51:Courbe ROC (LBP + SVM) 72
Figure 52:Courbe ROC (GLCM-LBP + SVM) 72
Figure 53:interface principale du système de détection de spam image 74
Figure 54:Description de l'interface 75
Figure 55:l'affichage de la classe 76

Liste des tableaux

Tableau 1 : Formulation mathématique des principaux descripteurs dérivés des GLCMs 49
Tableau 2: Tableau de confusion 64
Tableau 3 : Résultat de classification - dataset1 68
Tableau 4:Résultat de classification – dataset2 70
Tableau 5:Résultat de classification – dataset3 73

Liste des équations :

Équation 1:contraste C 33
Équation 2:la formule de la normalisation 43
Équation 3:normalisation de la matrice cooccurrence 46
Équation 4:contraste 46
Équation 5:Corrélation 46
Équation 6:Variance 46
Équation 7:Moment inverse 46
Équation 8:Somme moyenne 47
Équation 9:Somme variance 47
Équation 10:Somme entropie 47
Équation 11:Entropie 47
Équation 12:Différence de variance 47
Équation 13:Différence entropie 47
Équation 14:Mesure corrélation1 47

Équation 15:Mesure corrélation2 47
Équation 16:Mesure corrélation2 48
Équation 17:Le LBP d'un pixel c d'une image I 52
Équation 18:résultat LBP 52
Équation 19:formule de l'histogramme LBP 55

Table des sigles et acronymes

OCR	**: Optical Character Recognition.**
SVM	**: Support Vector Machine.**
KNN	**: K Nearest Neighbor.**
ML	**: Machine Learning.**
LBP	**: Local Binary Pattern.**
GLCM	**: Grey-Level Co-Occurrence Matrix.**
CNN	**: Convolutional Neural Network.**
URL	**: Uniform Resource Locator.**
GPU	**: Graphics Processing Unit.**

Introduction Générale

Aujourd'hui, le courrier électronique (e-mail) est devenu l'un des canaux le plus populaires, le plus puissants et plus fréquemment utilisés pour la communication personnelle et professionnelle en ligne Runbox, 2017. À titre indicatif, En 2015, le nombre d'utilisateurs de courrier électronique était de 2,6 milliards, tandis qu'en 2019, ce nombre passera à environ 2,9 milliards, avec plus d'un tiers de la population mondiale utilisant le courrier électronique pour échanger des messages Le nombre d'e-mails envoyés chaque jour dans le monde est de 293 milliards en 2019 (hors spams). Le succès de l'email est dû en partie à sa rapidité, sa permanence, son faible coût et la facilité de distribution des données.

Malgré ces avantages, le courrier électronique est confronté à un problème de sécurité majeur, à savoir la réception quotidienne par les utilisateurs d'un grand nombre de messages électroniques non sollicités, appelés "spams". Le spam est un courrier texte ou image indésirables et non sollicité reçu par les utilisateurs et souvent envoyé par un expéditeur obscur sans le consentement de l'utilisateur, qui peut souvent contenir des publicités, du contenu pour adultes, des logiciels malveillants, etc. L'utilisation répandue et massive du courrier électronique en fait une cible privilégiée pour les spammeurs. Le spam est devenu un problème majeur pour les réseaux Internet. Selon une étude récente de Symantec, indiquent que 90,4 % des e-mails incluent du contenu spam.

Aujourd'hui, la plupart des systèmes de courrier électronique sont dotés de mécanismes de filtrage de spams qui peuvent bloquer ou mettre en quarantaine les courriers indésirables, et la plupart d'entre eux sont essentiellement basés sur des technologies de filtrage du spam textuel. Dans ce contexte, de nombreux systèmes de classification ont été développés pour détecter et filtrer les courriers indésirables, en fonction d'un certain nombre de caractéristiques, telles que leur en-tête, leur objet et leur contenu. les auteurs exploitent quatre algorithmes d'apprentissage automatique utilisés pour détecter le spam en utilisant différentes parties du message électronique. Les algorithmes d'apprentissage automatique sont KNN, SVM, Naïve Bayes, etc. Ces classificateurs ont pu classer les spams textuels avec une précision d'environ 95 %. Par conséquent, au fil des années, la détection des spams basés sur le contenu est devenue très facile. Google, Microsoft, Yahoo ont utilisé des techniques qui fonctionnent très précisément pour classer les e-mails authentiques.

Pour contourner ces puissants filtres de détection basés sur le texte, les spammeurs ont réagi en introduisant de nouvelles techniques d'intégration de texte de spam dans des images jointes au courrier électronique, appelées "spam image". Le spam image est une sorte de spam dans lequel le texte du message est incorporé dans une image qui est ensuite jointes à l'e-mail. Les premiers spam images contenaient du texte facilement lisible, comme le montre la figure 1.3. Le texte spam intégré dans une image peut être une méthode efficace pour contourner les systèmes de filtrage textuelle Gao et al., 2008. Ce type de spam s'est rapidement développé ces dernières années, le défi majeur des nouveaux systèmes de filtrage est donc de trouver des méthodes efficaces pour distinguer une

image spam d'une image légitime (Ham) contenue dans l'email. Pour atteindre cet objectif, de nombreux travaux ont été réalisés en proposant des techniques pour filtrer ce type d'images contenues dans les e-mails. En général, les techniques de détection d'images spam sont divisées en trois catégories : i) Techniques basées sur l'en-tête de l'e-mail spam qui se compose de nombreux champs qui fournissent une gamme d'informations utiles pour l'analyse et la détection ii) Techniques basées sur l'OCR (Optical Character Recognition) qui utilisent la technique OCR pour extraire le texte intégré dans l'image Techniques non basées sur le contenu utilisant l'analyse du contenu de l'image et l'extraction de caractéristiques.

Les techniques basées sur l'OCR utilisent des techniques de reconnaissance optique de caractères pour extraire le texte intégré dans les images spam, puis le soumettre avec le corps du texte de l'e-mail à des techniques de détection basées sur le texte Nisha et Gaikwad, 2015. Récemment, pour contourner ce type de filtre anti-spam, les spammeurs ont introduit des techniques d'obscurcissement des images spam afin d'empêcher les outils OCR de lire le texte intégré dans les images. Cela a soulevé la question de l'amélioration de la détection du spam image à l'aide d'autres techniques. En particulier, plusieurs chercheurs ont étudié la possibilité d'utiliser des fonctionnalités d'image génériques de bas niveau pour reconnaître les images spam bruités.

Les techniques non basées sur le contenu sont destinées à étudier et analyser les caractéristiques et le contenu de l'image, tels que la couleur, la texture, le bord, l'ombrage, la surface, etc. sont extraits de l'image et qui sont utilisés pour filtrer les images spam.

Des recherches antérieures sur la détection du spam image ont montré que certains types de spam image peuvent être détectés avec une grande précision. Par exemple, les travaux présentés dans Annadatha & Stamp, 2018 ; Chavda, and al, 2018, une grande variété de propriétés d'image sont extraites et les images sont classées comme spam ou Ham (c'est-à-dire, images non-spam) basée sur des techniques d'apprentissage automatique. Cependant, certains types complexes de spam image sont difficiles à détecter à l'aide de ces techniques.

L'objectif de ce mémoire consiste à proposer un système de détection de spam image qui est capable de faire la distinction entre les images spam et les images légitimes (Ham) en se basant sur les caractéristiques de texture extraites de l'image. Nous proposons une méthode hybride pour l'extraction des caractéristiques des images en combinant deux méthodes, à savoir la méthode GLCM et la méthode LBP. De chaque image, deux types de caractéristiques sont extraits. La première méthode extrait les caractéristiques de texture de la matrice de cooccurrence des niveaux de gris (GLCM), tandis que la seconde méthode extrait les caractéristiques par la méthode modèle binaire local (LBP). Ensuite, pour classer les images en tant que spam ou non spam, nous réalisons une étude comparative se basant sur deux algorithmes d'apprentissage : Machine à Vecteur de support (SVM), et K Plus Proche Voisin (KNN). L'objectif principal est de sélectionner le meilleur algorithme pour classifier le courrier électronique reçu. Chaque classifieur a été utilisé de trois manières, avec les caractéristiques de texture de l'image extraites par la méthode GLCM, puis par la méthode LBP et enfin par la fusion de ces deux caractéristiques respectivement.

Nous prenons en compte à la fois les spams images du monde réel et les ensembles de données complexes de type spam images. Des tests expérimentaux seront réalisés sur une base de données réelle.

Ce mémoire est constitué en quatre chapitres, et organise comme suit :

- Dans le premier chapitre, nous présentons les concepts de base sur les spams en générale et les spams images en particulier et les différentes techniques utilisées pour détecter ce type de spam.
- Ensuite, le second chapitre détaille l'analyse de texture et les différentes approches utilisées.
- La conception de notre approche de détection de spam image est présentée dans le troisième chapitre.
- Le dernier chapitre est consacré à la description des différents outils utilisés dans le développement de notre application, ainsi que les différents résultats obtenus.
- Et enfin, nous terminerons ce mémoire par une conclusion générale et quelques perspectives.

Chapitre 1 : Détection et filtrage de spam image

1.1 Introduction

Aujourd'hui, le courrier électronique (e-mail) est devenu l'un des canaux le plus populaires, le plus puissants et plus fréquemment utilisés pour la communication personnelle et professionnelle en ligne. Malgré ces avantages, le courrier électronique est confronté à un problème de sécurité majeur, à savoir la réception quotidienne par les utilisateurs d'un grand nombre de messages électroniques non sollicités, appelés "spams". L'utilisation répandue et massive du courrier électronique en fait une cible privilégiée pour les spammeurs. Le spam est devenu un problème de sécurité majeur pour les réseaux Internet. De nombreuses solutions avaient été suggérées pour résoudre le problème.

Dans ce chapitre, nous présentons les concepts de base sur les spams en générale et les spam images en particulier et les différentes techniques utilisées pour détecter ce type de spam.

1.2 Notions sur le spam

1.2.1 Définition du spam

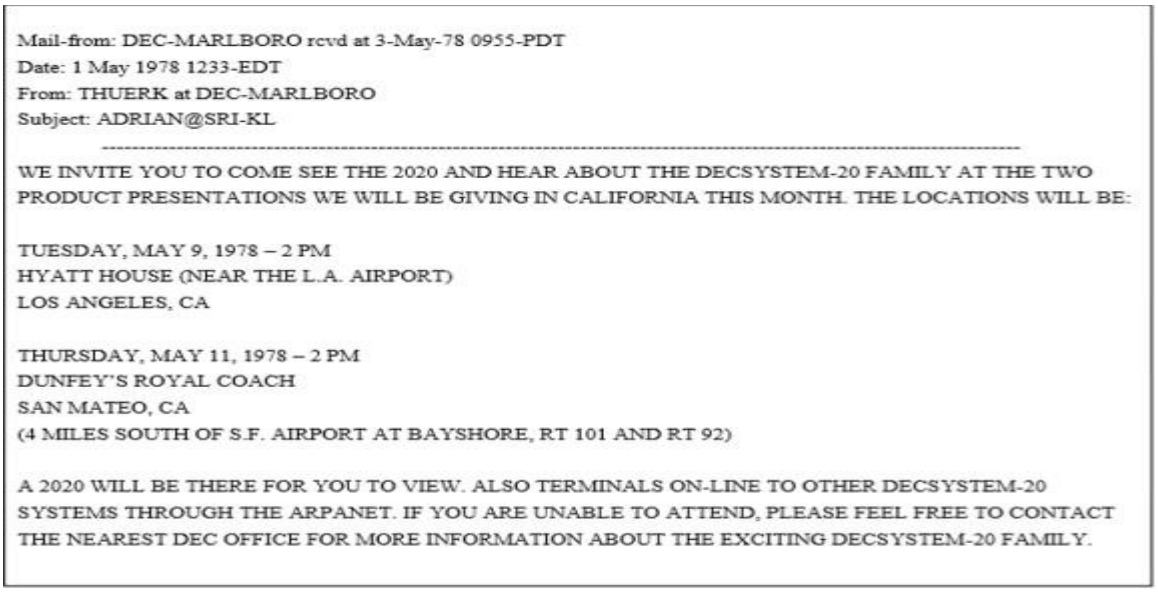
Le spam est un message électronique non sollicité, envoyé massivement à un grand nombre de destinataires, à des fins publicitaires ou malveillantes.

Le terme spam est aussi utilisé pour désigner le même type de message transmis par d'autres moyens de communication électroniques tels que les messageries instantanées, les blogs, les forums, et plus récemment, des réseaux de téléphonie mobile, via les SMS ou MMS. Même si le moyen de communication est différent, les techniques d'envoi et de détection restent relativement similaires.

Le premier spam (Figure 1) date du 3 mai 1978. Ce jour-là, sur le réseau ARPANET2, Gary Thuerk, commercial de la société informatique DEC3, invitait par e-mail 393 personnes à découvrir sa nouvelle machine, le 2020.

1.2.2 Types de spam

En plus des spams e-mail, il existe d'autres types de spam applicables à différents moyens de communication. Par exemple, les spams de messagerie sur téléphone mobile, ainsi que les spams des moteurs de recherche Web et les spams des réseaux sociaux (Dhanaraj & Karthikeyani, 2013).



Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT
Date: 1 May 1978 1233-EDT
From: THUERK at DEC-MARLBORO
Subject: ADRIAN@SRI-KL

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 – 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 – 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

Figure 1 : Premier spam sur le réseau ARPANET2, Gary Thuerk.

Spam d'e-mail est la forme de spam la plus répandue. Dans le spam par e-mail, les messages sont envoyés à un grand nombre d'adresses e-mail. Ces messages de spam peuvent inclure des publicités de produits, des liens vers des sites Web de phishing ou des liens vers des installateurs de logiciels malveillants. Historiquement, le spam par e-mail ne contenait que des messages texte. Au fur et à mesure que les filtres textuels s'amélioraient, les spams basés sur des images sont apparus comme un moyen de contourner ces filtres (Annadatha & Stamp, 2018). Il existe de nombreuses autres formes de spam par e-mail, y compris ce que l'on appelle le spam vierge, qui ne contient aucun message dans l'e-mail et est utilisé pour collecter des adresses email légitimes.

Spam de message de téléphone mobile (SMS) fait référence aux messages indésirables envoyés aux téléphones mobiles. De tels messages sont gênants pour les utilisateurs de téléphones mobiles, mais comme il y a des coûts associés au spam par SMS, il est moins courant que le spam par e-mail (Annadatha & Stamp, 2018).

Spam des moteurs de recherche fait référence aux mesures qui tentent d'affecter la position d'un site Web après une requête. En guise de contre-mesure, lorsqu'un site Web est détecté comme contenant du spam de moteur de recherche, le site est marqué et pénalisé. Une enquête a révélé que 51,3 % des piratages de sites Web étaient liés au spam des moteurs de recherche (Schwartz, 2018).

Spam des réseaux sociaux vise les sites Web de réseaux sociaux tels que Facebook et Twitter. Une technique de spamming social consiste à créer un faux compte dans une application sociale, qui est ensuite utilisé pour pirater des comptes d'utilisateurs valides. Ces faux comptes sont utilisés pour envoyer des messages en masse ou des liens malveillants, avec l'intention de nuire. À mesure que les sites de réseautage social sont devenus plus populaires, les activités de spam social telles que le clickbaiting ou le likejacking sont devenues plus courantes (Tolentino, 2015).

Spam de jeu consiste à envoyer des messages en masse aux joueurs en utilisant une salle de discussion commune ou une zone de discussion publique. Les spammeurs peuvent cibler les

utilisateurs qui aiment les jeux afin de vendre des articles de jeu contre de l'argent réel ou de la monnaie du jeu.

1.2.3 Objectifs des spam

Au départ, le spam visait principalement des objectifs publicitaires. Aujourd'hui, il s'est considérablement développé, diversifié et complexifié, pour atteindre de plus en plus souvent des objectifs malveillants. En effet, Le spam s'est non seulement développé en termes de volume, mais également en termes de contenu. Aujourd'hui, les objectifs des spam sont très variés en voici une liste non exhaustive :

- **Hameçonnage (ou phishing)** : L'objectif est de réussir à se faire passer pour un organisme connu par l'utilisateur, dans le but de lui voler des informations à caractère confidentiel. Par exemple, on reçoit un mail provenant "apparemment" de notre banque, ou d'un autre site où l'on dispose d'informations personnelles. Dans ce mail, il est demandé de cliquer sur un lien (pour des motifs divers : Réactualisation, etc.), après avoir cliqué sur ce lien, une page web s'affiche... sur laquelle il est demandé de rentrer ses coordonnées bancaires ou toute autre information personnelle. Parmi les sites Top les plus contrefaits pour les attaques de phishing, on retrouve eBay, Paypal et Bank of America.
- **Publicité** : L'objectif est de vanter les mérites d'un produit quelconque. Il s'agit par exemple de produits pharmaceutiques, de produits de luxe, de logiciels divers et variés, de jeux d'argent. Ils peuvent également soutenir-agate idées politiques, culturelles ou religieuses et / ou organisations.
- **Scam** : Il s'agit d'une attaque basée sur la naïveté des destinataires dans le but de leur soutirer de l'argent. L'exemple le plus courant est le scan nigérien : un dignitaire d'un pays d'Afrique vous demande de servir d'intermédiaire pour une transaction financière importante, en vous promettant un bon pourcentage de la somme. Pour amorcer la transaction, il vous faut donner de l'argent.
- **Canular** : L'objectif est de faire circuler une information semblant très sensible, souvent avec un caractère d'urgence : fausse alerte de virus, fausse alerte de contamination potentielle, chaine de solidarité…. Par exemple : « un nouveau virus très dangereux se propage, il faut faire circuler l'information »; « des sous-vêtements sont infectés par une dangereuse bactérie ».
- **Malware** : Est un logiciel conçu pour infiltrer ou endommager un système informatique. Il est communément pris pour contenir des virus informatiques, vers, chevaux de Troie, spywares et adwares. Ce type de logiciel est souvent envoyé en tant que non suspect d'une pièce jointe. Lorsque l'utilisateur ouvre le fichier, le logiciel malveillant s'installe. L'interdépendance entre les spams et les logiciels malveillants a évolué Spam logiciels malveillants propagation des e-mails, les logiciels malveillants est utilisé pour infecter un hôte de sorte que l'hôte peut être contrôlé à distance et utilisé pour l'envoi de plus de spams. Ces hôtes infectés sont désignés comme des « ordinateurs zombies ». Beaucoup

  De gens croient que la plupart des spams sont envoyés par des botnets, qui constituent un réseau de PC zombies.

1.2.4 Statistiques sur les spam

À titre indicatif, En 2015, le nombre d'utilisateurs de courrier électronique était de 2,6 milliards, tandis qu'en 2019, ce nombre passera à environ 2,9 milliards, avec plus d'un tiers de la population

mondiale utilisant le courrier électronique pour échanger des messages Le nombre d'e-mails envoyés chaque jour dans le monde est de 293 milliards en 2019 (hors spams). Selon le rapport du laboratoire Kaspersky, en 2015, le volume de spams envoyés a été réduit à son plus bas niveau en 12 ans. Le volume de spams est tombé en dessous de 50 % pour la première fois depuis 2003. En juin 2015, le volume de spams est tombé à 49,7 % et en juillet 2015, les chiffres ont encore été réduits à 46,4 % selon le développeur de logiciels antivirus Symantec. Cette baisse a été attribuée à la réduction du nombre de botnets majeurs responsables de l'envoi de spams par milliards. Le volume de spams malveillants a été signalé comme étant constant en 2015. Le nombre de spams détectés par Kaspersky Lab en 2015 se situait entre 3 et 6 millions. À l'inverse, alors que l'année touchait à sa fin, le volume de spams a augmenté. Un autre rapport de Kaspersky Lab a indiqué que les messages spam contenant des pièces jointes pernicieuses telles que des logiciels malveillants, des rançongiciels, des macros malveillantes et JavaScript ont commencé à augmenter en décembre 2015. Cette dérive s'est poursuivie en 2016 et en mars de la même année, le volume de spam avait quadruplé par rapport à celle observée en 2015. En mars 2016, le volume de spams découverts par Kaspersky Lab est de 22 890 956. À ce momentlà, le volume de spams avait grimpé en flèche pour atteindre une moyenne de 56,92 % pour le premier trimestre de 2016. Les dernières statistiques montrent que les spams représentaient 56,87 % du trafic de courrier électronique dans le monde et que les types de spam les plus connus étaient les soins de santé et spam de rencontres. Le spam entraîne une utilisation improductive des ressources sur les serveurs SMTP (Simple Mail Transfer Protocol) car ils doivent traiter un volume important de courriers électroniques non sollicités. Le volume de spams contenant des logiciels malveillants et d'autres codes malveillants entre le quatrième trimestre de 2016 et le premier trimestre de 2018 est illustré dans la figure 2 ci-dessous. Selon une étude récente de Symantec, indiquent que 90,4 % des e-mails incluent du contenu spam.

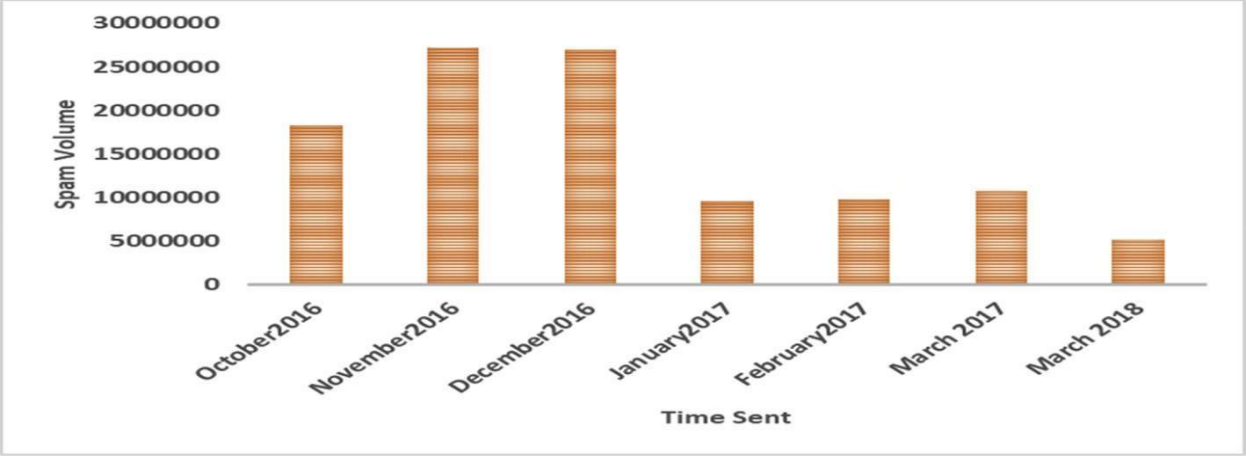


Figure 2:Le volume de spam emails du 4th quart 2016 to 1st quart 2018.

1.2.5 Impactes du spam sur les utilisateurs et les fournisseurs :

Dans cette section, nous présentons les effets du spam, au niveau des utilisateurs, entreprises.

1.2.5.1 Perte de temps

- Encombrement anormal des boîtes aux lettres.
- Suppression des courriels indésirables.
- Configuration et maintenance des filtres.
- Consultation des courriels rejetés pour y détecter les bons à cause du risque de passer à côté d'emails importants mal catalogués par les outils de détection anti-spam.

1.2.5.2 Perte de bande passante et d'espace disque

- Spécialement pour les utilisateurs de modems.
- Les pièces jointes des virus et spam peuvent être grands.

1.2.5.3 Pertes financières non négligeables aux niveaux des entreprises et FAI

- Une augmentation des coûts de gestion opérationnelle et support lié à la gestion anti spam.
- Perte de productivité des salariés, Selon une étude, le spam aurait coûté environ 712 $ par employé et par an aux entreprises. À ce chiffre, il faut rajouter 113 à 183 $ par employé et par an pour la gestion des emails en quarantaine.

1.3 Notions sur le spam image

1.3.1 Définition

Le spam image est une sous-classe du spam e-mail. Le spam image est une sorte de spam dans lequel le texte du message est incorporé dans une image qui est ensuite jointes à l'e-mail. Comme mentionné ci-dessus, le spam image est apparu comme une technique d'obscurcissement pour échapper aux filtres anti-spam textuels. Le spam image est généralement utilisé pour faire la publicité de produits, tromper les utilisateurs pour obtenir des données personnelles ou pour diffuser des logiciels malveillants (Dhanaraj & Karthikeyani, 2013). Il est plus difficile de détecter le spam image que le spam textuel et les techniques d'offuscation basées sur l'image peuvent être utilisées pour créer un spam image encore plus difficile que celui généralement observé dans la pratique (Annadatha & Stamp, 2018 ; Chavda et al. 2018). Des exemples de spam d'images du monde réel sont donnés dans les figures 3, 4 et 5.

1.3.2 Les types

Les e-mails basés sur le spam image sont vus dans différents e-mails de spam avec différentes formes. Les e-mails basés sur le spam image sont généralement classés en trois branches :

- L'e-mail spam image contient une image qui présente la cible du spammeur et une URL qui adresse l'image du site Web du spammeur. Dans ce cas, l'utilisateur après avoir reçu le courrier doit saisir l'URL dans la barre d'adresse pour visiter le site Web. L'image exploitée doit donc être suffisamment attrayante pour persuader l'utilisateur de le faire.

- Le contenu du spam image est similaire à tout le contenu utilisé dans les spams textuels. On peut dire que l'image utilisée est une capture d'écran du spam textuel habituel. Toutes les cibles sont visibles dans l'image avec tous les détails que le spammeur souhaite partager avec les utilisateurs. Par exemple, si le spammeur souhaite afficher des annonces dans le spam image, il peut contenir le nom du produit, la description du produit, le nom du producteur, l'adresse, le numéro de téléphone, etc.
- Le spam image est un lien hypertexte vers un site Web. L'utilisateur après avoir cliqué sur l'image peut voir le site Web spécial qui contient toute la description de la cible du spammeur avec des détails complets. En raison de la curiosité de l'utilisateur, le site Web hyperlié s'ouvrait généralement par un simple clic sur l'image.

Figure 3:Exemples de spam image (Yan Gao et al., 2008).

Figure 4:Exemples de spams images (i) financiers, (ii) produits, (iii) Internet et (iv) loisirs

Figure 5:Exemple d'image non spam de l'ensemble de données

1.3.3 Types de spam images

Le spam image a évolué au fil du temps et peut prendre plusieurs formes pour contourner les techniques anti-spam classiques. Les images utilisées pour le spam peuvent inclure des images textuelles, des images découpées et des images aléatoires, comme indiqué ci-dessous.

 Image texte uniquement : Le spam image de première génération consistait en des images contenant uniquement du texte. De telles images contiennent du texte pur intégré dans une image essentiellement vierge. Ces images ressemblent à des e-mails textuels, mais sont en réalité des images. La reconnaissance optique de caractères (OCR) peut être utilisée pour extraire ce texte, auquel cas des filtres traditionnels basés sur le texte peuvent être appliqués.


Hello,

You have been chosen to participate in an invitation only limited time event!

Are you currently paying over 3% for your mortgaged STOP! We can help you lower that today!

Answer only a few questions and we can give you an approval in under 30 seconds it is that simple!

And stop fighting for lenders, let them fight for you! Make them work for your business by giving you the lowest rates around! Two hundred and thirty thousand dollar loans are available for only three hundred and forty dollars/month!

WE ARE PRACTICALLY GIVING AWAY MONEY!

Think your credit is too bad to get a deal like this? THINK AGAIN! We will have you saving your money in no time!

Are you ready to save your money?
Regards

Figure 6:Spam image texte uniquement

 Image randomisée font référence à la randomisation des pixels de l'image. Pour créer une image aléatoire, les spammeurs modifient chaque pixel de l'image. les spammeurs ajoutent des bandes de couleurs aléatoires, des pixels colorés aléatoires, des nuances de couleurs. Par conséquent, il peut être difficile de distinguer l'image randomisée de l'image d'origine. Les modifications apportées n'affectent généralement pas sensiblement l'apparence de l'image, mais modifient les valeurs de hachage et peuvent même influencer les résultats des techniques de détection basées sur l'OCR.

Figure 7:Image avec pixel de couleur aléatoire

 Image obscurcie : L'obscurcissement est l'une des plus anciennes astuces dans ce domaine, par ex. mots mal orthographiés, rotation légère du texte, flou des contours du texte, ajout d'ombre et ajout de bruit aléatoire pour rendre l'image difficile à lire et empêcher la détection de plusieurs images similaires.

Figure 8:Exemples d'obscurcissement utilisés dans le spam d'image.

 Image découpée se compose de plusieurs images fusionnées à la manière d'un puzzle. Ce type de spam image est difficile à détecter et l'image combinée passe souvent par les filtres anti-spam d'image.

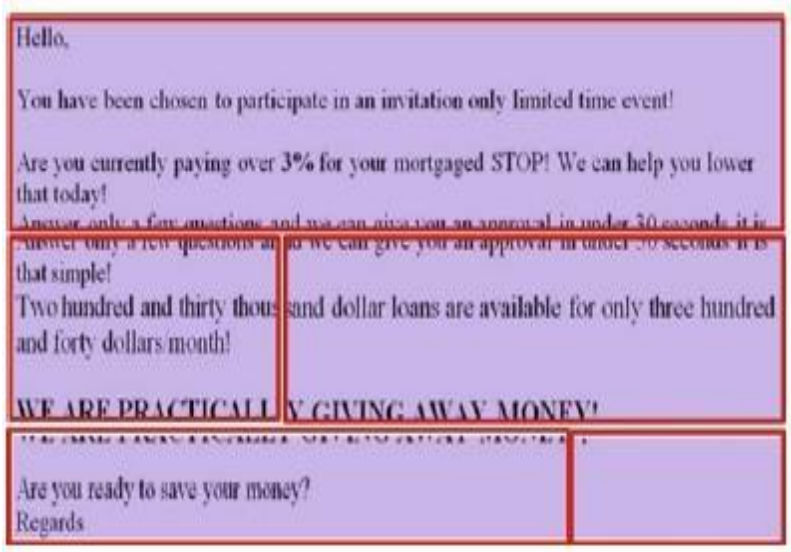


Figure 9:Image découpé

 Image avec fond sauvage : Les spammeurs utilisent des images avec des arrière-plans vagues et étranges. Ils utilisent des figures géométriques et des couleurs variées. Cette astuce cible l'OCR car l'OCR est normalement basé sur la mesure de la géométrie et recherche des formes géométriques similaires à des lettres et les place dans un fichier texte.

Toutes les méthodes qui utilisent l'OCR sont la cible de cette astuce.

Figure 10:Image avec fond sauvage.

 Images gif animées et en plusieurs parties : Les images sont divisées en plusieurs parties, certaines contenant le message et d'autres contenant une animation. Les cadres de l'image tournent assez rapidement pour n'afficher que le résultat final à l'utilisateur. Ceux-ci sont créés en combinant plusieurs images gif dans un seul fichier, affichées l'une après l'autre, donnant l'apparence d'un mouvement.

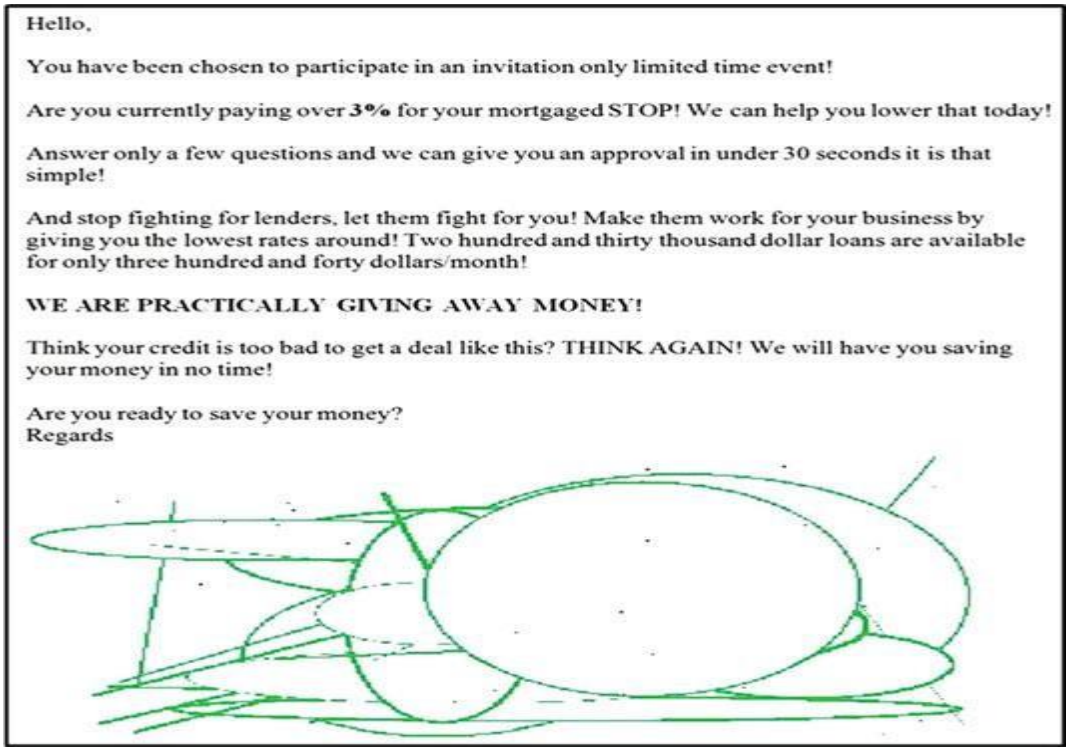


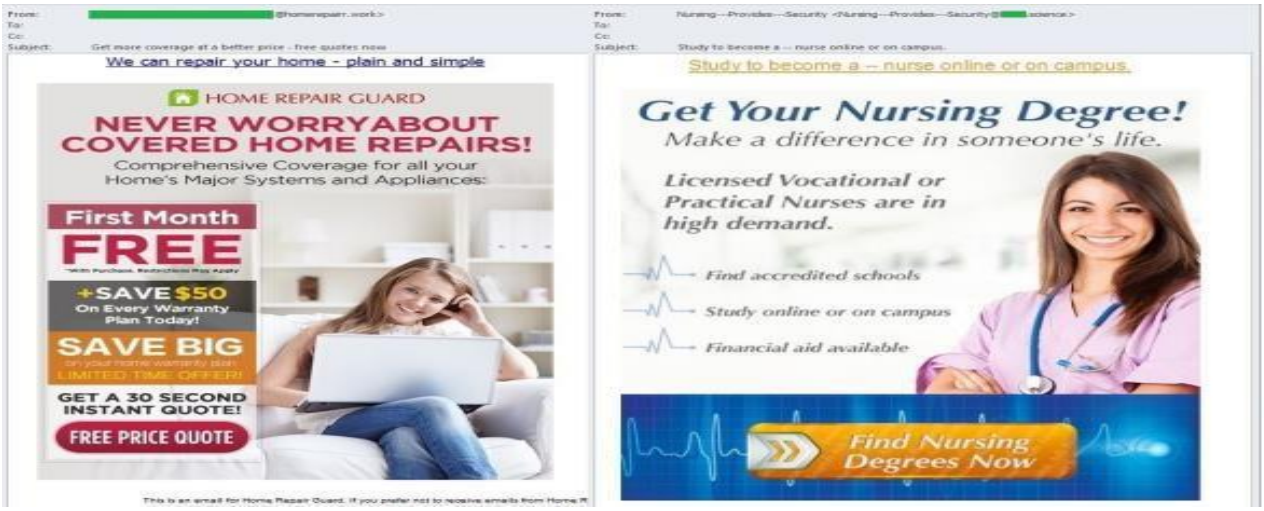
Figure 11:Exemple de spam image Gifs animés multi-images.

 Dessin animé : Cette nouvelle astuce utilise des polices de dessins animés qui sont inhabituelles et étranges pour le filtre anti-spam. Ils utilisent plusieurs couleurs, plusieurs styles et des formes

spéciales afin de produire un très bel artefact attrayant et perceptible pour l'homme, mais très difficile à détecter pour la machine.

Figure 12:Exemple de spam image de dessin animé.

 Images standard ou naturelle: Ce sont des images soignées, aucune des astuces ci-dessus n'est utilisée et cela lui donne un aspect authentique. Le message entier est contenu dans l'image et les filtres anti-spam ne peuvent donc pas le détecter. En fait, de nombreuses images qui arrivent aujourd'hui comme spam ont un aspect professionnel, ce qui les fait ressembler à des photographies.



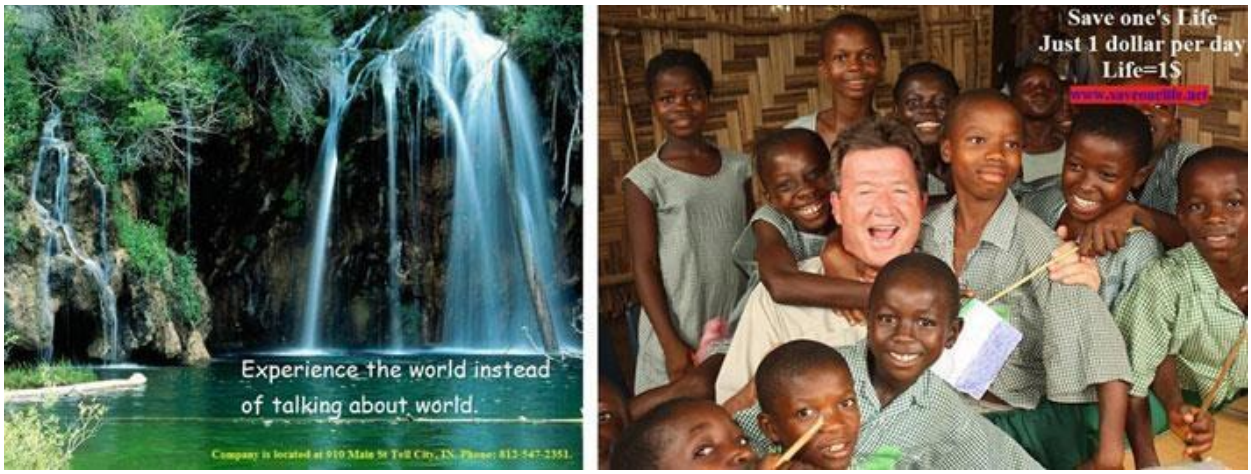


Figure 13:Exemple de spam images naturelles / standards.

1.3.4 Filtrage de spam image :

Dans ce qui suit, nous discutons de trois approches de détection de spam image. Plus précisément, nous considérons les techniques basées sur les en-têtes, les techniques basées sur le contenu et les techniques non basées sur le contenu. Notez que ces techniques ne sont pas mutuellement exclusives.

1.3.4.1 Techniques basées sur l'en-tête :

Aujourd'hui, les clients de messagerie modernes masquent souvent les en-têtes de la vue de l'utilisateur, c'est pourquoi de nombreuses personnes n'ont jamais vu d'en-tête de courrier électronique. Cependant, les en-têtes sont toujours livrés avec le contenu du message. La plupart des clients de messagerie offrent une option pour activer ou désactiver l'affichage de l'en-tête de l'e-mail. L'idée de ce groupe est d'analyser uniquement la partie en-tête des e-mails, car les messages électroniques contiennent plus qu'un simple message. L'en-tête de l'e-mail se compose de données sur l'expéditeur et le destinataire, y compris l'adresse e-mail de l'expéditeur, la date, de, à, etc. Les champs de l'en-tête de l'e-mail contiennent des informations précieuses qui peuvent être utiles pour distinguer le spam et le non-spam. Les attributs de l'entête de l'e-mail fournissent une gamme d'informations utiles pour l'analyse et la détection et ont été utilisés avec succès pour entraîner des modèles à détecter le spam (Hassanet al., 2017 ; Saraubon and Limthanmaphon, 2009 ; Liu et al. 2010). Ces techniques sont applicables au spam image. Certains des champs d'en-tête mentionnés sont utilisés dans la pratique et sont décrits cidessous :

1.3.4.2 Techniques basées le contenu :

Les filtres basés sur le contenu peuvent, par exemple, rechercher dans un e-mail des mots-clés particuliers qui se trouvent généralement dans le corps du message du spam. En règle générale, le corps d'un e-mail contient les informations réelles à fournir. Pour le spam image, les techniques basées sur l'OCR (Optical Character Recognition) peuvent être utilisé pour extraire le texte intégré dans l'image qui est ensuite transmis à un filtre basé sur le texte (Apache Software Foundation, 2018).Les techniques basées sur l'OCR utilisent des techniques de reconnaissance optique de caractères pour extraire le texte intégré dans les images spam, puis le soumettre avec le corps du texte de l'e-mail à des techniques de détection basées sur le texte (Nisha et Gaikwad, 2015 ; Dredze, et al, 2007). Récemment, pour contourner ce type de filtre anti-spam, les spammeurs ont introduit

des techniques d'obscurcissement des images spam afin d'empêcher les outils OCR de lire le texte intégré dans les images. Cela a soulevé la question de l'amélioration de la détection du spam image à l'aide d'autres techniques.

1.3.4.3 Technique non basée sur le contenu :

Les techniques non basées sur le contenu sont destinées à étudier et analyser les caractéristiques et le contenu de l'image, tels que la couleur, la texture, le bord, l'ombrage, la surface, etc. L'objectif est d'utiliser ces caractéristiques de l'image pour filtrer les spam image. Des recherches sur la détection de spam image ont montré que certains types de spam image peuvent être détectés avec une grande précision. Par exemple, les travaux présentés dans (Annadatha & Stamp, 2018 ; Chavda, and al, 2018), une grande variété de propriétés d'image sont extraites et les images sont classées comme spam ou Ham (c'est-à-dire, images non-spam) basée sur des techniques d'apprentissage automatique.

1.3.5 Travaux connexes

Depuis l'apparition des spam e-mails, la combinaison de techniques de traitement d'images et de techniques de classification a contribué au développement de systèmes de détection de spam image puissants. Certains travaux se concentrent sur la localisation de régions de texte dans une image spam, et d'autres utilisent différentes techniques permettant de distinguer les images légitimes (Ham) des images spam. Ci-dessous, nous passerons en revue les recherches pertinentes et récentes liées à notre travail.

Dhabi et al. (2020) ont proposé une méthode de filtrage de spam image basée sur l'algorithme de détection de région de texte. La méthode proposée est mise en œuvre en plusieurs phases. Premièrement, les transformées en ondelettes basées sur le niveau unique doivent trouver l'image d'entrée pour détecter les régions de texte candidates. Deuxièmement, un ensemble de caractéristiques fiables indiquant le spam sont extraites des régions de texte détectées.

Sharmin et al., (2020), ont proposé d'appliquer les réseaux de neurones convolutifs (CNN) au problème de détection du spam image et d'utiliser des CNN basés sur un nouvel ensemble de fonctionnalités qui est une combinaison de l'image brute et Canny edges.

Annadatha et al. (Annadatha & Stamp, 2018), utilise l'algorithme de classification SVM qui a été appliqué à un ensemble de 21 caractéristiques d'image. En utilisant une sélection de fonctionnalités basée sur des poids SVM linéaires, les auteurs sont en mesure d'atteindre un taux de précision de 0,97 avec un ensemble relativement petit de caractéristiques. Les auteurs fournissent un ensemble de données qui pourrait servir de spam image, mais qui est beaucoup plus difficile à détecter, par rapport au spam image du monde réel.

Chavda et al. (Chavda et al., 2018) mènent deux séries d'expériences avec SVM et traitement d'image. Les auteurs utilisent un ensemble complet de 41 caractéristiques d'image et ils obtiennent une précision de 0,97 et 0,98 sur deux ensembles de données accessibles au public. Ces auteurs fournissent également un ensemble de données, qui s'avère encore plus difficile à détecter que celui développé dans (Annadatha & Stamp, 2018).
Aiwan et al. (Aiwan & Zhaofeng, 2018) proposent une méthode de filtrage de spam image basée sur le réseau de neurones convolutifs (CNN). Le système proposé utilise l'augmentation des

données et réalise une amélioration de la précision, par rapport à des exemples sélectionnés de travaux antérieurs.

Kumar et al. (Kumar, R, & KP, 2018) appliquent des techniques d'apprentissage en profondeur au problème du spam d'image. Ils obtiennent une précision d'environ 91%, ce qui est comparable à d'autres recherches dans le domaine.

Chang (2017) a proposé un système de filtrage de spam image à trois couches. Le filtrage est effectué en analysant à la fois l'en-tête de l'image et l'image elle-même. La structure du modèle explique clairement l'idée de conception et les technologies liées au modèle. Les résultats expérimentaux montrent que le taux de classification est d'environ 93,0 %.

Hosseini et. Al (2015) a suggéré une méthode qui utilise les caractéristiques de texture d'image pour classer l'image de spam. Pour chaque image, la matrice de cooccurrence de niveaux de gris a été utilisée pour obtenir 22 caractéristiques, qui sont utilisées par le bayésien naïf et le k plus proche voisin (KNN).

Kumaresan et. al (2015) a proposé un schéma pour extraire les caractéristiques, en particulier les métadonnées et les caractéristiques d'histogramme des images. Sur la base de ces caractéristiques extraites, un classificateur SVM avec fonction noyau est utilisé pour détecter spam image. La complexité temporelle reste un problème pour cette méthode, mais la précision est de 90 %.

Chowdhury et al (2015) proposent une méthode qui extrait les métadonnées et les caractéristiques visuelles et les transmet au BPNN pour classification. Ils ont comparé trois algorithmes d'apprentissage automatique qui sont : SVM, Naïve Bayes et BPNN avec le même ensemble de fonctionnalités et sur le même ensemble de données.

Nisha D. Chopra et. al (2015) a proposé un système qui utilise deux méthodes pour classer les images spam. La première méthode utilise un outil OCR pour extraire le texte de l'image, et la seconde méthode utilise un classificateur bayésien pour détecter les spams.

Kumaresan et al. (Kumaresan, Sanjushree et Palanisamy, 2014) proposent une technique de détection de spam image basée sur les caractéristiques de couleur et utilisant l'algorithme *k*-plus proche voisin (K-NN). Plus précisément, les auteurs s'appuient sur les histogrammes RVB et HSV comme caractéristiques. Dans cette recherche, un classificateur simple K-NN donne une précision de 0,945.

Anand et. al (2012) présentent deux méthodes pour filtrer les spam image. La première méthode extrait les caractéristiques de bas niveau tandis que la seconde méthode extrait les caractéristiques de métadonnées de l'image. Les deux méthodes sont appliquées aux images contenant uniquement des zones de texte. Dans les deux procédés, les régions de texte sont extraites pour être entrées dans le système OCR.

Gao et al. (Yan Gao et al. 2008) proposent un schéma de détection de spam image qui s'appuie sur un algorithme d'arbre de boosting probabiliste. L'ingénierie des caractéristiques basée sur la couleur et l'histogramme du gradient orienté (HOG) est utilisée pour générer des vecteurs de caractéristiques pour cet algorithme d'apprentissage. Ces auteurs obtiennent une précision de 0,8944.

En plus des recherches qui traitent exclusivement les spam image, il existe de nombreux articles sur la détection de spam qui couvrent les aspects du problème de spam image. Par exemple, (Dada et al, 2019) réalise un et de l'art sur les articles de recherche traitant sur la détection de spam.

1.4 Conclusion :

Dans ce chapitre, nous avons présenté quelques concepts de base sur les spams en générale et les spams images en particulier avec leurs définitions, objectifs et impacts et sur les différentes techniques utilisées pour détecter ce type de spam.

Chapitre 2 : Analyse de la Texture

2.1 Introduction

L'analyse de texture est un domaine très important en traitement d'images. Parmis les principaux éléments d'interprétation du message visuel pour un observateur humain on peut citer les contours, la couleur, la forme, etc... L'analyse de l'image consiste souvent à extraire un certain nombre de propriétés caractéristiques et à les exprimer sous forme paramétrique. Les paramètres calculés permettent donc de décrire, de caractériser, de segmenter et d'analyser les images en question. Selon le cas, l'analyse peut être globale ou locale. Il est évident que le choix des paramètres dépend surtout de l'application considérée.

Le but peut être de lier par exemple ces paramètres avec les propriétés physiques et biologiques réelles afin de les quantifier ou alors de trouver des similitudes avec des textures de référence afin de les identifier. Il faut tout de même signaler que l'interprétation des informations dans un environnement naturel n'est pas un problème simple. En effet, les textures naturelles sont très irrégulières et ne peuvent être parfaitement modélisées par les techniques mathématiques actuelles.

Il n'existe pas de définition universelle pour la notion de texture, ce qui fait de l'analyse de texture une des problématiques les plus difficiles et d'actualité en traitement d'images. Intuitivement, la notion de texture est liée à l'aspect homogène d'une surface. Une des caractéristiques importantes de la texture, est son invariance à la translation.

L'analyse de texture est utilisée dans plusieurs applications : détection des objets, restauration des images, reconnaissance des manuscrits, compression d'image, segmentation, … etc.

2.2 Définition de l'image

Une image est plutôt difficile à décrire d'une façon générale. Une image est une représentation du monde. En traitement d'image, la majorité du temps, on considère qu'il s'agit d'une fonction mathématique de RxR dans R où le couplet d'entrée est considéré comme une position spatiale, le singleton de sortie comme l'intensité (couleur ou niveaux de gris) du phénomène physique. Il arrive cependant que l'image soit dite "3D" donc la fonction est de RxRxR dans R. Les images couleurs peuvent être représentées soit par trois images représentant les trois couleurs fondamentales, soit par une image de RxR dans RxRxR.

L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter.

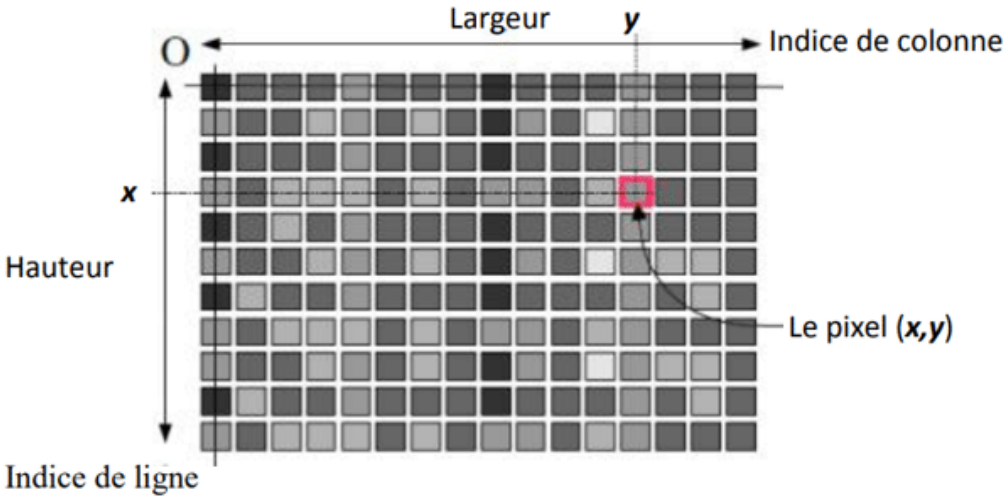


Figure 14:exemple d'image

2.3 Typologie d'image

Les formats d'images sont à diviser en deux grandes familles:

- **les images vectorielles** : elles sont utilisées pour stocker des objets géométriques (lignes, cercles... plus généralement courbes et polygones). Elles autorisent un stockage efficace et surtout permettent une restitution fidèle quel que soit le zoom appliqué à l'image Par contre ces formats sont peu appropriés pour représenter des images complexes et ne comportant pas de formes géométriques apparentes
- **les images matricielles** : consistait originellement à stocker sous forme d'un grand tableau les valeurs des pixels. On obtient des images matricielles à l'aide d'un appareil photo numérique, d'une caméra vidéo numérique ou d'un scanner. L'image peut être décomposé sous la forme d'une fonction f(x,y) de brillance analogique continue , définie dans un domaine borné ; tel que x et y sont les coordonnées spatiales d'un point de l'image et f une fonction d'intensité lumineuse ou de couleur, sous cet aspect , l'image est inexploitable par la machine ce qui nécessite sa numérisation.

2.4 Caractéristiques d'une image numérique

Comme nous l'avons vu, l'image est un ensemble structuré d'informations parmi ses caractéristiques nous pouvons citer les paramètres suivants :

Pixel

Une image numérique est constituée d'un ensemble de points appelés pixels (abréviation de Picture Elément) pour former une image. Le pixel représente ainsi le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image

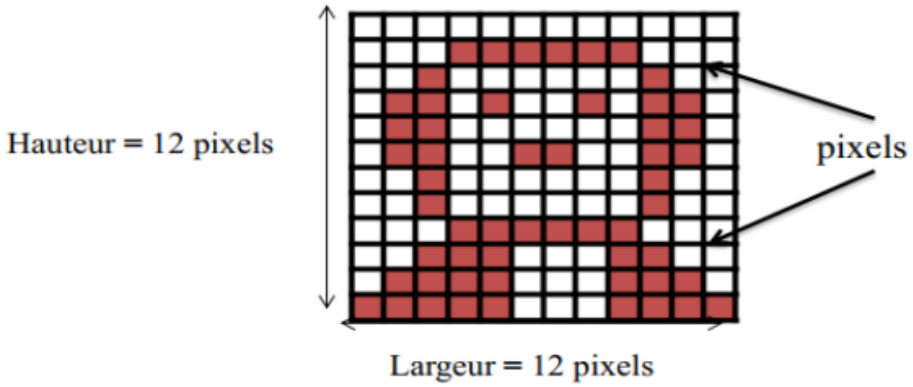


Figure 15:Groupe de pixel

La résolution

La résolution est définie par un nombre de pixels par unité de longueur de l'image à numériser en dpi (dots per inch) ou ppp (points par pouce). On parle de définition pour un écran et de résolution pour une image. Plus le nombre de pixels est élevé par unité de longueur, plus la quantité d'informations qui décrit l'image est importante et plus la qualité est meilleure (mais plus le poids de l'image est élevé). Autrement dit, la résolution d'une image correspond au niveau de détails qui vont être représentés sur une image.

Dimension

C'est la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multipliée par le nombre de colonnes nous donne le nombre total de pixels dans une image.

Bruit

Un bruit (parasite) dans une image est considéré comme un phénomène de brusque variation de l'intensité d'un pixel par rapport à ses voisins, il provient de l'éclairage des dispositifs de optiques et électroniques du capteur.

Figure 16:(a) Image sans bruit. (b) Image avec bruit

Contours

Les contours représentent la frontière entre les objets de l'image, ou la limite entre deux pixels dont les niveaux de gris représentent une différence significative. Les textures décrivent la structure de ceux-ci. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes.

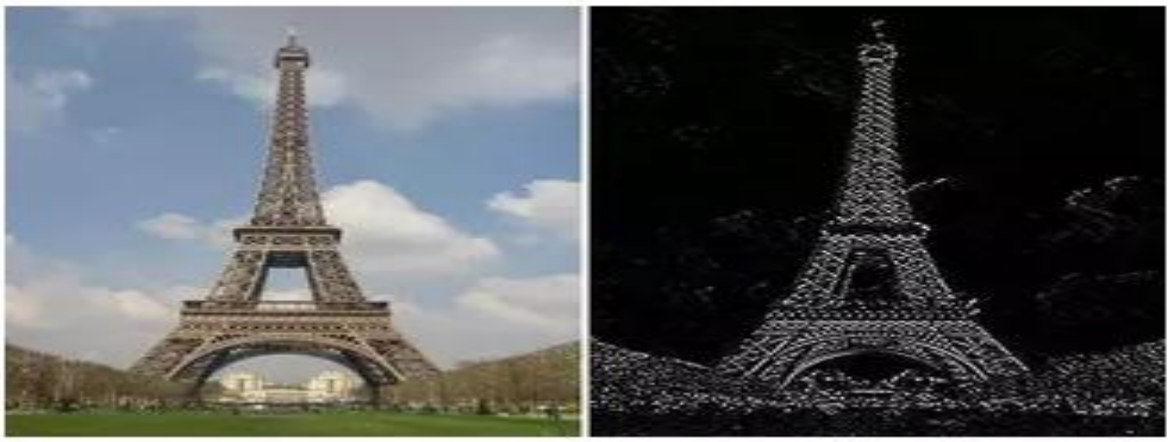


Figure 17:Contour d'une image.

La luminance

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, le mot luminance est substitué au mot brillance, qui correspond à l'éclat d'un objet.

Une bonne luminance se caractérise par :

- -Des images lumineuses (brillantes)
- -Un bon contraste : il faut éviter les images où la gamme de contraste tend vers le blanc ou le noir ; ces images entraînent des pertes de détails dans les zones sombres ou lumineuses.
- L'absence de parasites.

Histogramme

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris (couleur) et de voir entre quelles bornes est repartie la majorité des niveaux de gris (couleur) dans le cas d'une image trop claire ou d'une image trop foncée.

Il peut être utilisé pour améliorer la qualité d'une image (Rehaussement d'image) en introduisant quelques modifications, pour pouvoir extraire les informations utiles de celle-ci.

Pour diminuer l'erreur de quantification, pour comparer deux images obtenues sous des éclairages différents, ou encore pour mesurer certaines propriétés sur une image, on modifie souvent l'histogramme correspondant.

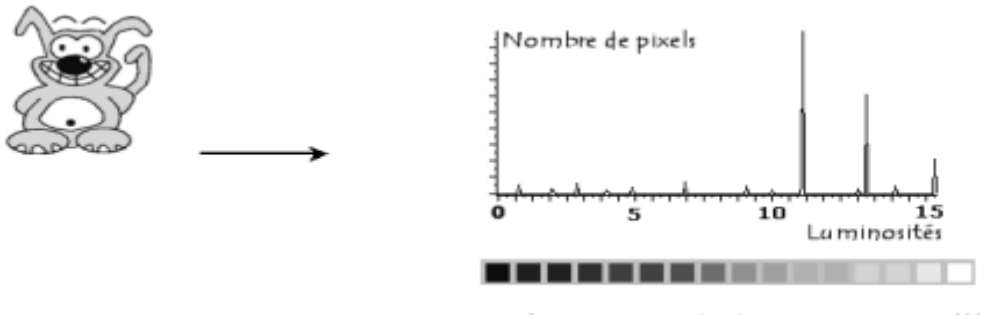


Figure 18:Image avec histogramme.

Le contraste

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'image.

Si L1 et L2 sont les degrés de luminosité respectivement de deux zones voisines A1 et A2 d'une

Image, le contraste C est défini par le rapport :

$$C = \frac{L1 - L2}{L1 + L2}$$

Équation 1:contraste C

2.5 Définition de la texture

La texture constitue un élément déterminant pour la vision humaine. C'est une des plus importantes caractéristiques utilisées pour identifier les différentes régions d'une image.

Il existe une multitude de travaux portant sur l'analyse de la texture, cependant il n'existe pas une approche formelle ou une définition précise de la texture (Coroyer, 1996). Unser, la définit comme suit: " Une texture est une région d'image pour la quelle il existe une fenêtre de dimension réduite, telle qu'une observation au travers de celle-ci se traduise par une impression ou perception visuelle, identique pour toutes les positions envisageables par translation à l'intérieur de la région considérée"(Coroyer, 1996).

Unser considère la texture comme une information visuelle, décrite par deux propriétés perceptuelles :

- La texture ne peut être définie que localement, c'est-à-dire, la taille du voisinage dépend de la taille des motifs la composant.
- La texture dépend de la résolution d'observation. A une certaine échelle, la même région d'une image, vue comme uniforme, peut paraitre une région texturée, en changeant la résolution d'observation.

Haralick, définit la texture comme étant un phénomène à deux dimensions :

- La répartition et la description spatiale des éléments de texture ou bien des éléments de base, appelées primitives, à partir des quels, elle est formée.
- La description des relations spatiales ou l'interaction entre ces primitives.

L'analyse de la texture, vise à extraire un ou plusieurs paramètres caractéristiques de la texture, appelés attributs texturaux.

La texture s'évalue à l'aide de l'ensemble des attributs texturaux, appelé descripteur de texture (Djerriri, 2004).

Un descripteur est défini comme la connaissance utilisée pour caractériser l'information contenue dans les images. Cette connaissance peut être acquise à partir d'études, d'expériences ou d'enseignements (Oanh, 2009).

Un descripteur de texture est une information qui permet de quantifier la répartition spatiale d'un motif dans l'image.

L'approche de caractérisation de la texture, à travers les descripteurs, diffère selon que la texture soit structurée ou désordonnée. Dans le cas des textures structurées, la caractérisation se fait souvent par une approche dite structurelle, basée sur l'utilisation de primitives et de règles de déplacement, décrivant les relations géométriques existant entre les primitives.

La texture structurelle, quant à elle, présente un aspect anarchique et désorganisé tout en gardant des caractéristiques locales typiques. Les primitives régulières ne pouvant pas être observées, la caractérisation des textures structurées se fait généralement par approche statistique, qui repose sur une description stochastique des propriétés caractérisant un voisinage (Djerriri, 2004).

Gagalowicz propose une synthèse des deux approches, en définissant la texture comme une structure spatiale constituée par l'organisation de primitives ayant chacune un aspect aléatoire (Gagalowicz, 1983).

2.5.1 Types de texture

Selon l'aspect visuel, la texture peut être répartie en trois types: les textures périodiques, les textures aléatoires et les textures hybrides.

Texture périodique

Une texture périodique est formée de primitives arrangées d'une façon spécifique. Le motif de base se répète de manière régulière. Il s'agit d'une texture ordonnée (Figure 19).

Figure 19:Exemples de textures ordonnées

Texture aléatoire

Une texture aléatoire semble totalement désordonnée, où Il est impossible d'isoler un motif de base (Figure 20).

Figure 20:Exemples de textures aléatoires

Texture hybride

Une texture hybride possède simultanément le caractère déterministe et aléatoire stochastique (Figure 21).

Figure 21:Exemples de textures hybrides

Les spécialistes utilisent un catalogue d'images représentant différents types de textures (Figure22). Ces images sont considérées comme une base de référence, pour valider les différentes méthodes d'analyse de texture.

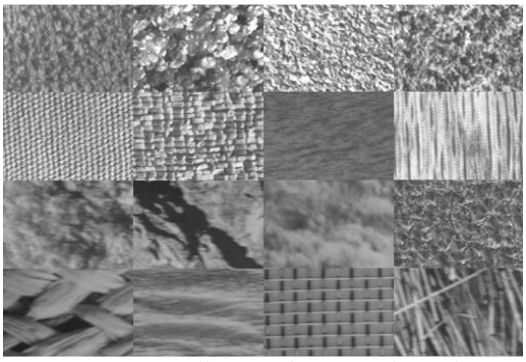


Figure 22:Base d'images de texture de Brodatz

Terminologie

Ci-dessous, quelques notions concernant l'analyse de texture.

A. Elément textural

Haralick définie l'élément textural comme étant le plus petit ensemble élémentaire dans lequel on ne décèle plus aucune variation de la caractéristique prise en compte pour un niveau de perception donné (Mohand, 2008).

B. Structure

Une structure est définie comme étant l'organisation de répartition des éléments texturaux au sein d'un élément de paysage (Zahzah, 1992).

C. Primitive de texture

Elle est définie par Haralick comme étant un ensemble de points de texture donnée, cet ensemble devant être maximum et connexe. Une telle primitive doit être telle que son continu soit homogène selon un critère donné, et le contenant doit être défini de façon géométrique et probabiliste (Djerriri, 2004).

La Figure 23 illustre le principe de primitive. A gauche, la primitive correspond à une brique. A droite, elle correspond à un pixel.

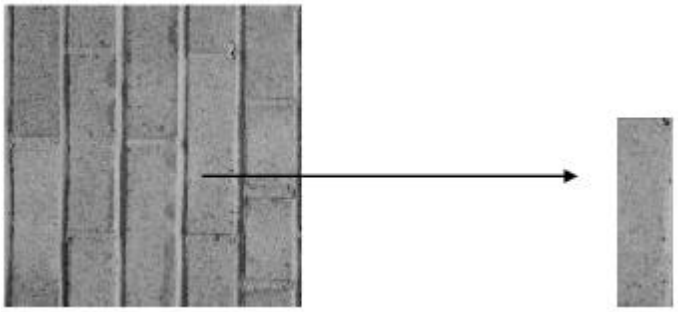


Figure 23:Primitive et échelle d'observation

D. Signature de texture

La signature de texture est une représentation formelle des caractéristiques de texture. Elle doit être calculable, pertinente et représentative (Zahzah, 1992).

E. Résolution de texture

La résolution de texture est la taille minimale de fenêtre laissant les mesures de textures invariantes (Djerriri, 2004).

F. Invariance par translation

Une texture présente à une échelle donnée, le même aspect quelque soit la zone observée. Ainsi, les statistiques calculées, sont invariantes à la translation (Djerriri, 2004).

G. Echèle d'observation

L'évaluation d'une texture dépend du niveau d'observation. Des textures fines peuvent être considérées comme grossières à un niveau d'analyse différent (Figure 2.5).

2.6 Analyse visuelle de la texture

L'oeil humain distingue en moyenne 16 niveaux de gris différents, du noir au blanc. Il est capable de discriminer des différences de niveaux de gris de 2%.

Le pouvoir séparateur de l'oeil est de 1 minute d'angle maximum, ce qui correspond à deux points séparés de 150 microns, vus à une distance de 40 cm. Il existe une zone de l'espace, à laquelle l'oeil n'est pas sensible. De ces faits, une image ne peut être parcourue en une seule fois, une décomposition en plusieurs parties est faite instinctivement (Djerriri, 2004).

Julesz a mené des études expérimentales sur la discrimination visuelle de la texture, dans le but de modéliser le système de vision humaine. Il a conclu que lors de l'analyse d'une image, l'observateur recherche des indices lui permettant de repérer les différentes textures présentent dans une image. Instinctivement, une analyse macroscopique est faite, pour analyser les contours des différentes régions homogènes apparentes dans l'image, chaque région est alors considérée comme une texture. Ensuite, une analyse plus fine est réalisée afin de repérer les caractéristiques de chaque texture (Djerriri, 2004).

2.7 Méthodes d'analyse de texture

Les méthodes d'analyse de textures servent à quantifier les différentes textures présentent dans une image. Ces techniques d'analyse ont un pouvoir discriminatif meilleur que celui de l'ensemble oeil-cerveau, qui est moins sensible aux variations complexe de texture.

Les méthodes d'analyse de textures peuvent être classées en quatre catégories.

2.7.1 Méthodes basées sur un modèle de texture

Ces méthodes se basent sur un modèle pour représenter le signal. Le modèle est défini par un certain nombre de paramètres qui caractérisent la texture. Les mêmes modèles sont souvent utilisés dans la littérature. La différence se situe dans le paramétrage ainsi que les algorithmes de segmentation et de classification utilisés.

Les modèles les plus utilisés sont les champs de Markov. Les méthodes basées sur ce modèle, font l'hypothèse que la valeur de niveau de gris du pixel considéré ne dépend que d'un voisinage réduit du pixel, en supposant que tout le passé du processus est contenu dans ce même voisinage. Plusieurs travaux ont porté sur les chaines de Markov, Si-Tayeb (2009) a fusionné un modèle de Markov avec les réseaux de neurones, pour la classification des images satellites (Si-Tayeb , 2009) . Kadar (2010) a proposé un modèle Markovien, pour la détection des changements dans les images satellites (Kadar, 2010).

2.7.2 Méthodes structurelles

Ce sont les méthodes d'analyse texturale fondées sur la description de primitives et sur la formalisation des relations spatiales entre ces primitives. Ces techniques partent du principe que les textures ordonnées possèdent des primitives qui se répètent dans les images en différentes dispositions, suivant une certaine loi.

L'analyse commence par l'identification des éléments constitutifs, puis la définition des règles de placement. Les structures les plus importantes sont les graphes et les structures syntaxiques. Dans le cas des structures syntaxiques, une signature ordonnée de la texture est décrite par un arbre dont les éléments texturaux représentent les noeuds. Une grammaire est associée à cet arbre qui décrit la nature et la forme. La recherche de structures identiques se fait en parcourant l'image, après une étape d'apprentissage, qui permet la description de la texture recherchée, en termes de grammaire d'arbre (Zahzah, 1992).

2.7.3 Méthodes statistiques

Ce sont des méthodes très utilisées pour l'analyse de texture. Elles se basent sur des évaluations quantitatives de la distribution de niveau de gris, en étudiant les relations entre un pixel et ses voisins. Les méthodes statistiques sont utilisées généralement pour caractériser des structures fines sans régularité apparente. L'ordre de la statistique, renseigne sur le nombre de pixels pris en considération dans le calcul des paramètres (Mohand, 2008).

A. Méthodes statistiques du premier ordre

Ces méthodes sont basées sur les histogrammes de premier ordre (histogramme d'intensité). Un tel histogramme indique la fréquence d'apparition d'un niveau de gris dans un voisinage considéré. Plusieurs paramètres statistiques de degrés différents peuvent être extraits à partir de l'histogramme. Parmi les statistiques fréquemment utilisées pour décrire une texture, il y a la moyenne, la variance, l'énergie et l'entropie (Tonye et al., 2000).

B. Méthodes statistiques du deuxième ordre

La limitation des méthodes du premier ordre, réside dans le fait que les paramètres calculés ne tiennent compte que de l'histogramme de l'image. Or, Deux images différentes, donc de textures différentes, peuvent avoir le même histogramme. Il est donc indispensable d'intégrer des informations concernant la localisation du pixel, et ne pas se contenter du nombre de niveaux de gris dans l'image. Il s'agit de passer à une méthode d'analyse de texture, d'ordre statistique supérieur. Parmi ces méthodes, il y a: les matrices de cooccurrence, la fonction d'auto-corrélation, le spectre de texture, les longueurs de plage…etc (Djerriri, 2004).

2.7.4 Méthodes basées sur le filtrage

Les études faites sur le système humain de vision, ont montré que l'image perçue par le cerveau, est décomposée en versions filtrées, ce qui a amené les chercheurs à s'intéresser à l'analyse de texture multi-canal (Abadi, 2009).

Le principe des méthodes d'analyse de texture à base de filtre, appelées aussi méthodes fréquentielles, est d'extraire l'énergie portée par le signal dans de différentes bandes de fréquences. La texture est considérée comme un mélange de signaux de fréquences, d'amplitudes et de différentes directions.

Parmi les techniques d'analyse de texture basées sur les filtres, citons : les ondelettes, le spectre de puissance de Fourier, la morphologie mathématique et le filtre de Gabor.

Une décomposition de l'image en ondelettes, consiste à effectuer en premier un codage en sous bandes, chacune des sous-images, représente l'image initiale à différentes résolutions. La résolution constitue un paramètre important, car pour chaque variation, de nouvelles textures peuvent apparaitre. Des mesures d'énergie ou d'entropie, sont ensuite calculées pour chaque sous image. Enfin, la discrimination de la texture se fait en définissant une distance (Djerriri, 2004).

Quant au spectre de puissance de Fourrier, l'idée est d'opérer des changements de représentation du domaine spatiale au domaine fréquentiel, ce qui permet de représenter les textures par des concentrations d'énergie dans le spectre de Fourier, traduisant une périodicité horizontale et verticale (Materka, 2001).

La morphologie mathématique consiste à transformer une image à l'aide des opérations : érosion, dilatation, ouverture et fermeture en déplacent un élément structurant sur l'image, ce qui permet

de discriminer différents types de textures. Belmadani (2000) a utilisé la morphologie mathématique pour la détection des modes dans les images satellites (Belmadani, 2000).

2.8 Notions d'attribut et de descripteur de texture

L'étude de la texture des objets d'une image peut avoir des objectifs très divers : obtenir des informations sur la nature d'un objet, segmenter l'image en régions homogènes, améliorer la qualité de l'image (restauration), identifier la texture afin de la réduire à un ensemble de paramètres (compression d'images) etc…

La discrimination et l'analyse de la texture nécessitent l'extraction d'un ou de plusieurs paramètres caractéristiques de cette texture. Nous désignerons ces paramètres sous le terme d'attributs texturaux ou indices (en anglais : textural features) et l'ensemble qu'ils constituent sous le terme de descripteur de texture. Certains de ces paramètres correspondent à une propriété visuelle de la texture.

Les attributs texturaux peuvent être obtenus à partir d'un ensemble assez vaste de différentes théories mathématiques.

2.9 Conclusion

La texture est un concept facile à reconnaitre, mais difficile à définir. Il n'existe pas de définition complètement satisfaisante.

Les méthodes d'analyse de textures peuvent être classées en quatre catégories : les méthodes statistiques, les méthodes de filtrage, les méthodes structurelles et les méthodes fondées sur un modèle.

Il n'existe pas une méthode d'analyse type, qui discrimine tous les genres de textures.
Le descripteur de texture une fois calculé, est soumis au processus de classification. Cette tache sera détaillée dans le chapitre suivant

Chapitre 3 : Conception

3.1 Introduction

L'objectif de ce mémoire consiste à proposer un système de détection de spam image qui est capable de faire la distinction entre les images spam et les images légitimes (Ham) en se basant sur les caractéristiques de texture extraites de l'image. Nous proposons une méthode hybride pour l'extraction des caractéristiques des images en combinant deux méthodes, à savoir la méthode GLCM et la méthode LBP. De chaque image, deux types de caractéristiques sont extraits. La première méthode extrait les caractéristiques de texture de la matrice de cooccurrence des niveaux de gris (GLCM), tandis que la seconde méthode extrait les caractéristiques par la méthode LBP. Ensuite, pour classer les images en tant que spam ou Ham, nous réalisons une étude comparative se basant sur deux algorithmes d'apprentissage : Machine à Vecteur de support (SVM), et K Plus Proche Voisin (KNN). L'objectif principal est de sélectionner le meilleur algorithme pour classifier le courrier électronique reçu. Nous prenons en compte à la fois les spams images du monde réel et les ensembles de données complexes de type spam images. Des tests expérimentaux seront réalisés sur une base de données réelle.

Dans ce chapitre nous décrivons en détaille la conception du modèle proposé en donnant les détails de chaque module de la conception.

3.2 Architecture générale du système

La Figure en bas illustre l'architecture conceptuelle de notre système proposé. Nos recherches sur la détection de spam image nous permettent de constater que toutes les solutions proposées pour résoudre ce problème sont construites selon les mêmes architectures globales, fonctionnant en trois modules principaux indépendants :

- Prétraitement et normalisation
- Extraction des caractéristiques
- Classification

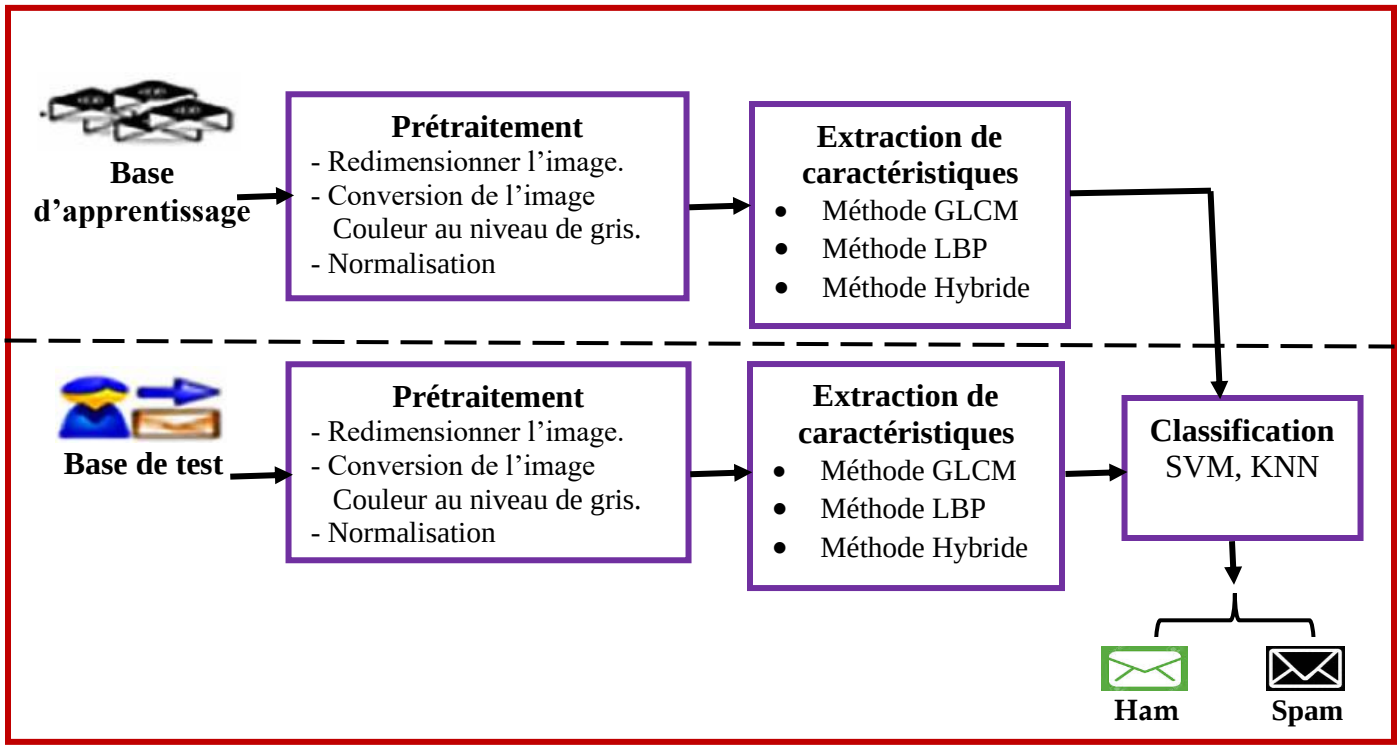


Figure 24 : Architecture générale

3.2.1 Ensemble de données

Ce projet utilise la combinaison de trois ensembles de données différents :

- **Dredze Image Spam Dataset :**(Dredze et al. 2007) ont créé un ensemble de données contient 3 ensembles d'images. Ham personnel (PHam) contient 2 021 images dont 1 517 sont uniques. Personal Spam (PSpam) contient 3 298 images, dont 1 274 sont uniques. Enfin, les archives de spam (SpamArch) contiennent 16 028 fichiers de différents formats (JPEG, PNG, GIF, etc.), dont 3 039 images uniques. En outre, l'archive de spam contenait beaucoup de fichiers non traités dans différents formats tels que gif, txt, jpg, etc
- **Image Spam Hunter (ISH)** (Gao et al. 2008) : Ce dataset contient à la fois des images spam et ham au format JPEG qui sont collectées à partir des e-mails originaux. Il y a 810 images ham et 929 images spam au total. Le nombre d'images uniques de spam et de ham est de 879 et 810 respectivement.
- **Improved Dataset** (Annadatha, 2019) : Ce dataset a été créé par Aneri et al, en effectuant une transformation sur les images ham pour les faire ressembler à des spam. Les images ham ont été redimensionnées à la taille des images spam pour aligner leurs caractéristiques de métadonnées. Du bruit a été introduite dans les images spam pour rendre difficile la détection des bords, puisque les images spam ont généralement moins de bruit que les images ham. Le nombre d'images uniques dans ce jeu de données est de 975. Il est disponible à l'adresse.

Nous avons également prétraité et combiné ces ensembles de données pour en construire un seul ensemble de données qui contient 1585 images spam et 659 images ham pour l'apprentissage et 377 images spam et 151 images ham pour le test. Ensuite, les expériences ont été réalisées sur cet ensemble de données.

3.2.2 Prétraitement

Le prétraitement est une étape importante dans le processus de filtrage des images spam. Le prétraitement est la technique qui vise principalement à réorganiser les données et à réduire ou éliminer les données de bruit et à ne conserver que les informations importantes pour rendre l'opération suivante (processus d'extraction de caractéristiques et classification) facile à mettre en œuvre. En général, l'étape de prétraitement comprend les opérations suivantes.

3.2.2.1 Unification du format et de la taille d'image des images

Les images de spam et ham dans l'ensemble de données existent dans différents formats (BMP, PNG, JPEG, GIF, TIFF, etc.) et tailles. Par conséquent, afin de faciliter la mise en œuvre du processus d'extraction de caractéristiques ainsi que du processus de classification, nous avons décidé de :

- Unifiez les différents formats d'image en JPEG, car c'est l'un des formats d'image les plus populaires et les plus efficaces.
- Redimensionnez toutes les images à la même taille (par exemple 65 × 65).

3.2.2.2 Convertir des images colorées en une image en niveaux de gris

Une image en niveaux de gris est simplement une image dans laquelle les seules couleurs sont des nuances de gris. Contrairement aux images couleur, ces types d'images nécessitent moins d'informations fournies pour chaque pixel et sont tout à fait suffisants pour de nombreuses tâches où il n'est pas nécessaire d'utiliser des images couleur plus difficiles à traiter. En fait, la couleur "grise" est une couleur dans laquelle les composantes rouge, verte et bleue ont toutes les mêmes valeurs d'intensité, il est donc nécessaire de spécifier pour chaque pixel une seule valeur d'intensité, contrairement aux images couleur qui nécessitent trois intensités pour chaque pixel. L'image en niveaux de gris est représentée par la luminance en utilisant la valeur 8 bits donnant 256 différentes

nuances de gris possibles du noir au blanc. Convertir une image couleur en une image en niveaux de gris consiste simplement à convertir les valeurs RVB (24 bits) en valeurs en niveaux de gris (8 bits). Dans le modèle RGB, si R, G et B désignent respectivement la valeur de couleur Rouge, Vert et Bleu, la valeur de gris peut être obtenue à l'aide de l'équation suivante :

RVB = (0,299 x R) + (0,587 x G) + (0,114 x B)

3.2.2.3 Normalisation

La normalisation est un processus considéré comme un élément de prétraitement de l'information essentiel pour garantir que les propriétés dans les portées numériques plus importantes ne dominent pas celles des portées numériques plus petites. La normalisation dans le traitement d'image est le processus qui modifie la plage de valeurs d'intensité des pixels. La normalisation est parfois appelée étirement du contraste ou étirement de l'histogramme. Il existe plusieurs façons de normaliser, mais la plus simple et la plus largement utilisée est la normalisation min-max, qui est l'une des façons les plus courantes de normaliser les données.

Supposons que : $I : \{X \subseteq \mathbb{R}^n\} \rightarrow \langle Min, \dots, Max \rangle$ and $IN : \{X \subseteq \mathbb{R}^n\} \rightarrow \langle newMin, \dots, newMax \rangle$

La normalisation est la transformation d'une image en niveaux de gris à n dimensions (I) dont les valeurs d'intensité sont dans la plage (Min, Max), en une nouvelle image (IN) dont les valeurs d'intensité sont dans la plage (newMin, newMax). La normalisation d'une image numérique en niveaux de gris s'effectue par la formule suivante :

Équation 2:la formule de la normalisation

$$IN = (I - Min)\frac{newMax - newMin}{Max - Min} + newMin$$

3.2.3 Extraction des caractéristiques

Une fois la phase de prétraitement terminée, le processus d'extraction de caractéristiques est appliqué à l'image. L'extraction de caractéristiques est l'une des phases les plus importantes de notre système, qui vise à extraire les propriétés caractéristiques d'une image et à les exprimer sous forme de vecteur de caractéristiques (f_0, f_1, f_2,…,f_n). La représentation qui en résultera servira de base à l'étape suivante, qui est la classification. Actuellement, il existe de nombreuses méthodes d'extraction de caractéristiques différentes, certaines d'entre elles peuvent réussir dans certains cas et échouer dans d'autres. Dans notre travail, nous nous intéressons aux méthodes du second ordre, plus précisément nous choisissons la méthode de la matrice de cooccurrence de niveaux de gris (GLCM) et la méthode LBP. Ces méthodes sont largement utilisées dans l'analyse de texture d'image.

3.2.4 Méthode de la Matrice de cooccurrence des niveaux de gris

La matrice de cooccurrence de niveaux de gris (GLCM) est l'une des méthodes d'extraction de caractéristiques de texture les plus anciennes et les plus importantes proposées par Haralick (Haralick, 1979). Depuis lors, cette méthode a été largement utilisée dans de nombreux domaines de l'analyse de texture. À partir des GLCM, plusieurs caractéristiques sont extraites par Haralick pour caractériser la texture.

3.2.4.1 A. Principe général

Les matrices de cooccurrence sont analogues à des histogrammes bidimensionnels. Elles représentent le nombre d'occurrence de couples de pixels particuliers dans l'image. La principale

caractéristique des matrices de cooccurrence est de s'intéresser à des couples de pixels qui sont, par définition, séparés par une distance (1, 2, 3,4…).

Le calcul d'une matrice de co-occurrence de niveaux de gris ou GLCM (Grey Level Co-occurrence Matrix) consiste à repérer dans une image le nombre d'occurrences de paires de niveaux de gris séparés par une distance d dans une direction définie par un vecteur de déplacement (dx,dy) [Haralick et al., 1973].

La matrice de cooccurrence exprime la probabilité d'apparition du couple de niveau de gris (i, j) de l'image dans une fenêtre et une direction donnée. Elle est basée sur le calcul de la probabilité qui représente le nombre de fois où un pixel de niveau de gris apparait à une distance et une direction d'un pixel de niveau gris.

La matrice de cooccurrence *Mc* (*i*, *j*) est carrée et de dimension *L*×*L*, où *L'*est le nombre de niveaux de gris présents dans *B*. Les indices de la matrice de cooccurrence sont donc les niveaux de gris de la texture étudiée. La matrice *Mc* (*i*, *j*) se construit comme suit :

1. Initialisation de la matrice *i*, *j* ∀ [0, *L* [: *Mc* (*i*, *j*) = 0.

2. Remplissage de la matrice. Si la relation *R* entre deux pixels (*x*1, *y*1) et (*x*2, *y*2) est respectée :

Mc (f (x1, y1), f (x2, y2)) = MC (f (x1, y1), f (x2, y2)) + 1

Dès lors, *Mc* (*i*, *j*) contient le nombre de fois que l'on a rencontré dans *B* deux pixels (*x*1, *y*1), (*x*1, *y*1) vérifiant la relation géométrique *R* et tel que *f* (*x*1, *y*1) = *i* et *f* (*x*2, *y*2) = *j*. En pratique, on utilise des relations géométriques assez simples comme celle citée comme exemple. Ainsi, on définit une matrice orientée

$$P_{90^\circ},\ d(i,\ j)\ =\ (x_1,\ y_1),\ (x_2,\ y_2)\ \in\ B\ x_1 = x_2, |y_2 - y_1| = d,\ f(x_1, y_1) = i\ \text{ et }\ f(x_2, y_2) = j$$

90° = correspond à une direction verticale.

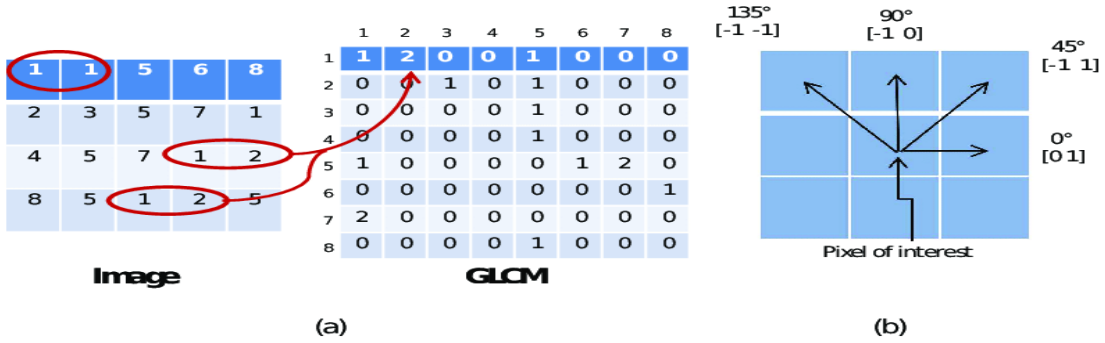
d = détermine la distance entre les deux pixels.

$$P_{0^\circ},\ d(i,j) = (x_1, y_1), (x_2, y_2)\ B\ \ x_1 = x_2, |y_2 - y_1| = d,\ \ f(x_1, y_1) = i\ \text{ et }\ f(x_2, y_2) = j$$

0° =correspond à une direction verticale.

d = détermine la distance entre les deux pixels.

Observation : Il est également possible de définir d'autres matrices correspondant aux directions 45° et 135°.



Un exemple sur la matrice de cooccurrence :

Soit l'image suivante comportant $L = 4$ niveaux de gris ($l = 0, 1, 2, 3$) :

$Mc(x, y)$ est la matrice de cet image :

$$Mc(x, y) = \begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 2 & 2 & 3 \\ 2 & 2 & 3 & 3 \end{matrix}$$

Les matrices $P0°, 1$ et $P90°, 1$ sont donc de dimension 4 et valent

$$P_{0°,1} = \begin{bmatrix} 6 & 2 & 1 & 0 \\ 2 & 2 & 0 & 0 \\ 1 & 0 & 4 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix} \qquad P_{90°,1} = \begin{bmatrix} 6 & 1 & 2 & 0 \\ 1 & 2 & 1 & 1 \\ 2 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

On peut remarquer que les matrices de cooccurrence sont bien symétriques.

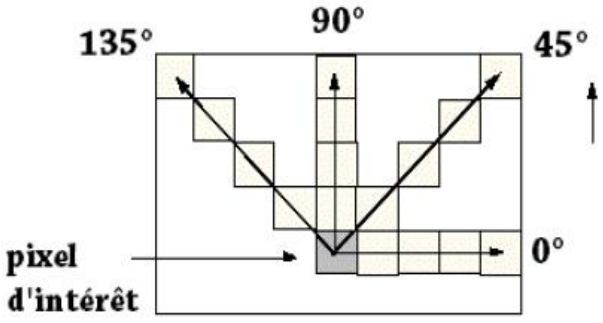


Figure 25:Exemples des directions de la matrice de cooccurrence

Pour le calcul des caractéristiques basées sur le GLCM, il est donc essentiel de normaliser la matrice GLCM pour obtenir une sorte de matrice de probabilité. L'opération consiste à diviser chaque entrée de la matrice par la somme de toutes les entrées. Les caractéristiques de texture sont calculées sur la base de la moyenne des quatre matrices de cooccurrence directionnelles. Dans notre travail, nous avons considéré la distance θ = (0°,45°,90°,135°) et d =1.

Nous avons normalisé la matrice de cooccurrence comme suit : pour chaque couple, *Mc(i, j)* est calculé selon l'équation (3) suivante :

Équation 3:normalisation de la matrice cooccurrence

$$Mc(i,j) = \frac{P(i,j)}{\sum_i \sum_j Mc(i,j)}$$

3.2.4.2 Caractérisation statistique des textures

Les matrices de cooccurrences GLCM (G, d, θ), contiennent les moyennes d'espace du premier ordre. Plusieurs indices ont été proposé par Haralick qui correspondent à des caractères descriptifs des textures peuvent être calculés à partir de ces matrices. Haralick a proposé 14 paramètres de textures calculés à partir des matrices de cooccurrence, pour extraire l'information texturale contenue dans l'image (Haralick, 1973). La plupart des paramètres de Haralick ont une signification visuelle.

Energie ou second moment angulaire:

Équation 4:contraste

$$f_1 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} P_{(i,j)}^2$$

Contraste:

Équation 5:Corrélation

$$f_2 = \sum_{k=0}^{Ng-1} k^2 \left(\sum_{i=1}^{Ng} \sum_{j=1}^{Ng} P_{(i,j)} \right)^{|i-j|=k}$$

Corrélation:

Équation 6:Variance

$$f_3 = \frac{1}{\sigma^2} \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} (ij) P_{(i,j)} - \mu^2$$

Variance:

Équation 7:Moment inverse

$$f_4 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} (i - \mu^2) P_{(i,j)}$$

Moment inverse:

Équation 8:Somme moyenne

$$f_5 = \sum_{i=1}^{Ng}\sum_{j=1}^{Ng}\frac{P_{(i,j)}}{1+(i-j)^2}$$

Somme moyenne:

Équation 9:Somme variance

$$f_6 = \sum_{k=0}^{2Ng-2} k\, P_{x+y}(k)$$

Somme variance:

Équation 10:Somme entropie

$$f_7 = \sum_{k=0}^{2Ng-2} (k-f_6)^2\, P_{x+y}(k)$$

Somme entropie:

Équation 11:Entropie

$$f_8 = -\sum_{k=0}^{2Ng-2} P_{x+y}(k)\log\left[P_{x+y}(k)\right]$$

Entropie:

Équation 12:Différence de variance

$$f_9 = -\sum_{i=1}^{Ng}\sum_{j=1}^{Ng} P_{(i,j)} log\left[P_{(i,j)}\right]$$

Différence de variance:

Équation 13:Différence entropie

$$f_{10} = \sum_{k=0}^{Ng-1}\left[P_{|x-y|}(k)(k-\sum_{l=0}^{Ng-1} l\, P_{|x-y|}(k))^2\right]$$

Différence entropie:

Équation 14:Mesure corrélation1

$$f_{11} = -\sum_{k=0}^{2Ng-2} P_{x-y}(k)\log\left[P_{x-y}(k)\right]$$

Mesure corrélation1:

Équation 15:Mesure corrélation2

$$f_{12} = \frac{f_9 - HXY1}{H}$$

Mesure corrélation2:

Équation 16:Mesure corrélation2

$$f_{13} = \sqrt{1 - e^{[-2*|HXY2 - f_9|]}}$$

Maximum corrélation coefficient:

f_{14} Représente la racine carrée de la deuxième plus grande valeur propre de *Qi*

$$Q(i,j) = \sum_k \frac{p(i,k)p(j,k)}{p_x(i)p_y(k)}$$

Tels que :

$$p_{x+y}(k) = \sum_{i=1}^{Ng}\sum_{j=1}^{Ng} P_{(i,j)} \qquad \begin{matrix} k = i + j \\ k = 0,1,2..Ng \end{matrix}$$

$$p_{|x-y|}(k) = \sum_{i=1}^{Ng}\sum_{j=1}^{Ng} P_{(i,j)} \qquad \begin{matrix} k = |i - j| \\ k = 0,1,2...Ng \end{matrix}$$

$$P_{(i)} = \sum_{i=1}^{Ng} P_{(i,j)} \qquad \mu = \sum_{g=1}^{Ng} gP_{(g)} \qquad \sigma^2 = \sum_{g=1}^{Ng} P_{(g)(g-\mu)^2}$$

$$HXY1 = -\sum_{i=1}^{Ng}\sum_{j=1}^{Ng} P_{(i,j)} log\ [P_{(i)}P_{(j)}]$$

$$HXY2 = -\sum_{i=1}^{Ng}\sum_{j=1}^{Ng} P_{(i)}P_{(j)}\ log\ [P_{(i)}P_{(j)}]$$

$$H = \sum_{i=1}^{Ng} P_{(g)}\ log\ [P_{(g)}]$$

Bien que les GLCMs fournissent une description riche de la dépendance spatiale, il est peu pratique de les manipuler sous leur forme brute. Haralick a ainsi proposé un ensemble de 14 descripteurs statistiques ou attributs permettant de résumer l'information texturale contenue dans les GLCMs (Haralick et al., 1973). Cependant, seul un sous-ensemble parmi ces 14 descripteurs est régulièrement utilisé. En compilant une série de publications traitant de la classification de textures, on peut identifier les 5 descripteurs d'Haralick apparaissant le plus souvent dans la littérature. Il s'agit de l'énergie, l'entropie, le contraste, la corrélation et l'homogénéité. Par ailleurs, d'autres descripteurs que ceux définis par Haralick peuvent également être dérivés des GLCMs. Il s'agit entre autres de la dissimilarité, autre descripteur d'ordre deux proche du contraste, ainsi que de descripteurs d'ordre supérieur à deux tels que le cluster shade et le cluster prominence. Il est à noter que la moyenne et la variance telles que définies par Haralick (soit la moyenne et la variance des entrées de la GLCM pour le pixel de référence) sont aussi régulièrement combinées aux autres descripteurs. La formulation mathématique définissant l'ensemble de ces descripteurs est présentée dans le Tableau 1.

Tableau 1 : Formulation mathématique des principaux descripteurs dérivés des GLCMs

Energie	$\sum_i \sum_j P_{i,j}^2$	Homogénéité	$\sum_i \sum_j \frac{P_{i,j}}{1+(i-j)^2}$
Entropie	$\sum_i \sum_j P_{i,j}(-\ln P_{i,j})$	Corrélation	$\sum_i \sum_j P_{i,j}\left[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{\sigma_i^2 \sigma_j^2}}\right]$
Contraste	$\sum_i \sum_j P_{i,j}(i-j)^2$	Cluster Shade	$\sum_i \sum_j P_{i,j}(i-\mu_i+j-\mu_j)^3$
Dissimilarité	$\sum_i \sum_j P_{i,j}\lvert i-j\rvert$	Cluster Prominence	$\sum_i \sum_j P_{i,j}(i-\mu_i+j-\mu_j)^4$

Tableau 1 : Formulation mathématique des principaux descripteurs dérivés des GLCMs

Où $P_{i,j}$ = probabilité d'occurrence de la paire de niveaux de gris i, j (GLCM normalisée),

$\mu_i = \sum_i i P_{i,j}$, la moyenne des entrées normalisées pour le pixel de référence de valeur i,

$\mu_j = \sum_j j P_{i,j}$, la moyenne des entrées normalisées pour le pixel voisin de valeur j,

$\sigma_i = \sum_i P_{i,j}(i-\mu_i)^2$, l'écart-type des entrées normalisées pour le pixel de référence de valeur i,

$\sigma_j = \sum_i P_{i,j}(j-\mu_j)^2$, l'écart-type des entrées normalisées pour le pixel voisin de valeur j.

La signification statistique des descripteurs présentés dans le Tableau 1 peut être décrite comme suit :

- L'**énergie** exprime le caractère régulier de la texture. De manière générale, une énergie élevée est observée lorsque l'image est très régulière, c'est-à-dire lorsque les valeurs élevées de la GLCM sont concentrées à quelques endroits de la matrice. C'est le cas par exemple pour des images dont la distribution des niveaux de gris a soit un aspect constant, soit un aspect périodique. Une image aléatoire ou fortement bruitée produit une GLCM distribuée de manière plus uniforme et présente une énergie faible.
- Le **contraste** est plus élevé pour des GLCMs présentant des valeurs plus larges en dehors de la diagonale, autrement dit pour des images affichant des changements locaux d'intensité. La **dissimilarité** exprime les mêmes caractéristiques de l'image que le contraste à la différence que le poids des entrées de la GLCM augmente linéairement en s'éloignant de la diagonale plutôt que quadratiquement dans le cas du contraste. Ces deux descripteurs sont dès lors souvent corrélés.
- L'**entropie** est d'autant plus élevée que la diagonale de la GLCM est étalée, le cas extrême étant une GLCM uniforme. En ce sens, l'entropie est l'inverse de l'énergie et caractérise l'aspect irrégulier de l'image, d'où une corrélation forte entre ces deux attributs.

- L'**homogénéité** évolue à l'inverse du contraste et prend des valeurs élevées si les différences entre les paires de pixels analysées sont faibles. Celle-ci est donc plus sensible aux éléments diagonaux de la GLCM, contrairement au contraste qui dépend plus des éléments éloignés la diagonale.

- La **corrélation** peut s'apparenter à une mesure de la dépendance linéaire des niveaux de gris dans l'image.
- Le **cluster shade** et le **cluster prominence** donnent des informations sur le degré de symétrie de la GLCM. Plus ceux-ci sont élevés moins la GLCM est symétrique. La symétrie s'entend ici au sens de symétrie globale de la GLCM et pas uniquement de symétrie par rapport à la diagonale de la matrice. De plus, si le cluster prominence est faible, cela signifie qu'un pic existe autour de la moyenne des valeurs de la GLCM et donc qu'il y a peu de variations de niveaux de gris dans l'image.

Une fois calculés et éventuellement normalisés, l'ensemble des descripteurs sont rassemblés dans un vecteur unique caractérisant chaque pixel ou chaque région de l'image. Ce vecteur d'attributs peut ensuite être utilisé comme donnée d'entrée dans un classifieur. Dans le cas d'une analyse pixel-à-pixel, les descripteurs sont souvent représentés sous la forme d'une image pour chaque descripteur calculé.

3.2.4.3 Calcul des paramètres

Le calcul des paramètres de Haralick se déroule comme suit:

Faire glisser une fenêtre de taille n, en la centrant sur chaque pixels appartenant à l'image. La matrice de cooccurrence est calculée à partir de cette fenêtre, en prenant en compte une direction θ et une distance d. Dans le but de discriminer le maximum de texture, toutes les directions sont prises en considération. Quatre matrices de cooccurrences associées aux orientations 0°,45°,90°, 135° sont calculées. Pour chacune d'entre elles, le paramètre de texture souhaité est calculé, Puis la moyenne des valeurs obtenues est effectuée. Le résultat obtenu est renvoyé à l'image de texture correspondant au paramètre choisi, aux mêmes coordonnées du pixel central en cours (centre de la fenêtre). L'opération est refaite pour tout pixel appartenant à l'image initial à niveaux de gris, et pour chacune de ses bandes.

Afin d'éviter les effets de bord, un remplissage des points de bordure, selon le principe de symétrie, est réalisé avant le début de calcul.

Dans le cadre de ce travail, les paramètres les plus courants dans la littérature, sont utilisés, à savoir : l'énergie, le contraste, l'entropie, et le moment inverse (Boudali, 2010). **(**Abid , 2012**)**.

3.2.4.4 Réglage des paramètres

Une des difficultés majeures rencontrées lors de l'utilisation des GLCMs est le réglage des paramètres. Celui-ci est en effet difficilement automatisable et doit s'adapter au cas par cas aux caractéristiques du motif constituant la texture à analyser. Cet aspect est aussi à mettre en relation avec la résolution spatiale de l'image. Les paramètres à fixer sont la distance entre paires de sites, l'orientation du déplacement, le degré de quantification des niveaux de gris, la taille de la fenêtre d'analyse et le choix des descripteurs texturaux. Une approche régulièrement employée dans cette phase de paramétrisation est de tester différentes combinaisons de ces paramètres afin d'identifier la combinaison la plus optimale. Ces éléments sont discutés ci-dessous

3.2.5 La méthode des motifs binaires locaux (LBP : local binary pattern)

3.2.5.1 Le LBP de base

L'opérateur LBP a été proposé initialement par Ojala et al. (Ojala et al., 1996) dans le but de caractériser la texture d'une image. Le calcul de la valeur LBP consiste pour chaque pixel à seuiller ses huit voisins directs avec un seuil dont la valeur est le niveau de gris du pixel courant.

Tous les voisins prendront alors une valeur 1 si leur valeur est supérieure ou égale au pixel courant et 0 si leur valeur est inférieure (Figure 26). Le code LBP du pixel courant est alors produit en concaténant ces 8 valeurs pour former un code binaire. On obtient donc, comme pour une image à niveaux de gris, une image des valeurs LBP contenant des pixels dont l'intensité se situe entre 0 et 255.

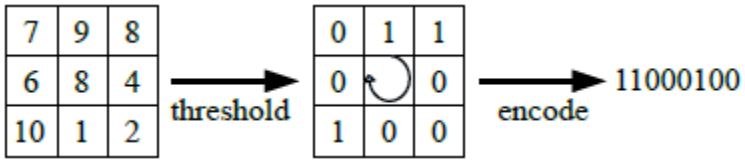
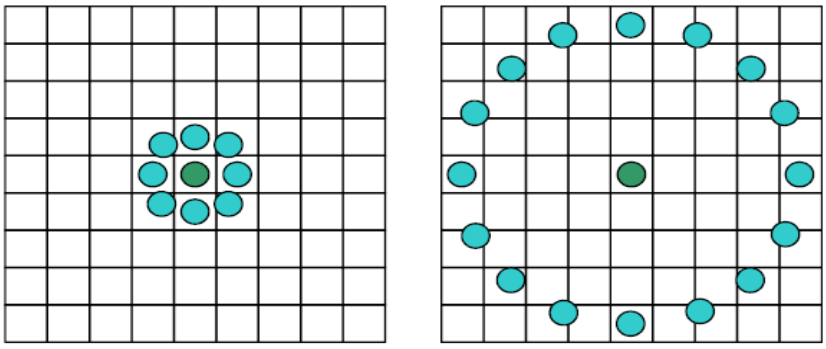


Figure 26:Opérateur LBP.

La technique LBP a été étendu ultérieurement en utilisant des voisinages de taille déférente. Dans ce cas, un cercle de rayon R autour du pixel central et Les valeurs des P points échantillonnés sur le bord de ce cercle sont prises et comparées avec la valeur du pixel central. Pour obtenir les valeurs des P points échantillonnés dans le voisinage pour tout rayon R, une interpolation est nécessaire. On adopte la notation (P, R) pour définir le voisinage de P points de rayon R d'un pixel. La (Figure 26), illustre deux voisinages pour des valeurs de R et P différentes.



N=8, R=1 *N=16, R=4*

Figure 27:Exemples de voisinages utilisés pour le calcul des LBP.

Les différentes valeurs possibles de motifs peuvent être assimilées à des microtextons à différentes échelles, au sens où les primitives ainsi mesurées correspondent à des lignes, à des zones uniformes ou encore à des points, voir figure 27.

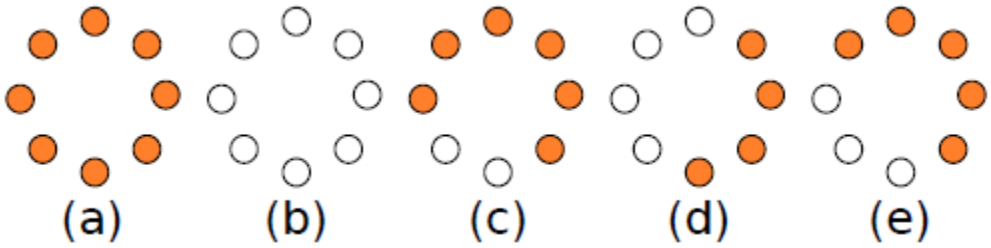


Figure 28:Primitives extraites par les motifs binaires locaux.

(a) et (b) correspondent à des taches respectivement claires et sombres, (c) est une fin de ligne, (d) une bordure et (e) est un coin.

Le LBP d'un pixel c d'une image I, pour un voisinage de rayon R avec P points, est défini comme:

$$\forall_c \in \mathbb{N}^2,\ \forall P \in \mathbb{N},\ \forall R \in \mathbb{R},\ LBP_{P,R} = \sum_{P=0}^{P-1} s\left(I_R(p) - I(c)\right) * 2^p$$

Équation 17:Le LBP d'un pixel c d'une image I

Où :

$$\forall_x \in \mathbb{R},\ s(x) = \begin{cases} 1 & si \quad x \geq 0 \\ 0 & sinon \end{cases},$$

$$\forall_{(x_c, y_c)} \in \mathbb{N}^2,\ \forall P \in \mathbb{N}, \forall_p \in \{1..P\},$$

$$I_R(p) = I\left(x_c + Rcos\left(2\pi\frac{p}{P}\right), y_c - Rsin\left(2\pi\frac{p}{P}\right)\right)$$

Équation 18:résultat LBP

3.2.5.2 LBP uniforme

L'extension suivante des LBP concerne la définition des motifs uniformes qui permettent de réduire la taille du vecteur de description et de rendre les LBP invariants par rotation. En effet, le nombre de motifs possibles augmente rapidement avec le nombre de voisins pris en considération. Par exemple, pour 16 voisins, l'histogramme aura une taille de 216 = 65536 dimensions, ce qui est inutilisable dans une application réelle. (Maenpa, 2000) suggèrent de ne considérer que les motifs n'ayant qu'un faible nombre de transitions. Cette modification a été inspirée par le fait que certains motifs apparaissent plus souvent que d'autres et donc concentrent plus d'informations utiles. Le nombre de transitions U d'un LBP est défini comme:

$$U\left(LBP_{P,R}\right) = \left|s\left(I_R(p-1) - I(c)\right) - s\left(I_R(0) - I(c)\right)\right| + \sum_{p=1}^{P-1} \left|s(I_R(p) - I(c)) - \ s(I_R(p-1) - I(c))\right|$$

Les motifs uniformes les plus utilises, nommés uniformes 2, correspondent à ceux ayant deux transitions après seuillage ou moins (donc U ≤ 2). Par exemple, le label 00000111 (deux transitions)

est uniforme 2 alors que 01101101 (six transitions) ne l'est pas. Les motifs non uniformes sont tous conserves sous le même label. La taille du vecteur de caractéristiques passe alors de 2*P* éléments à P (P − 1) + 3. Par exemple, la description avec un voisinage de huit voisins contient normalement 256 labels différents, parmi lesquels 58 sont uniformes. Cela permet de réduire la taille du vecteur de description à 59 valeurs. Il a été montré par (Ojala et al., 2002) que les motifs uniformes 2 comptabilisent généralement près de 90 % de l'information de texture contenue dans l'image.

L'utilisation d'un code LBP uniforme, noté LBP^{u2} à deux avantages. Le premier est le gain en mémoire et en temps calcul. Le deuxième est que LBP^{u2} permet de détecter uniquement les textures locales importantes, comme les spots, les fins de ligne, les bords et les coins (Figure 28, b), pour des exemples de ces textures particulières.

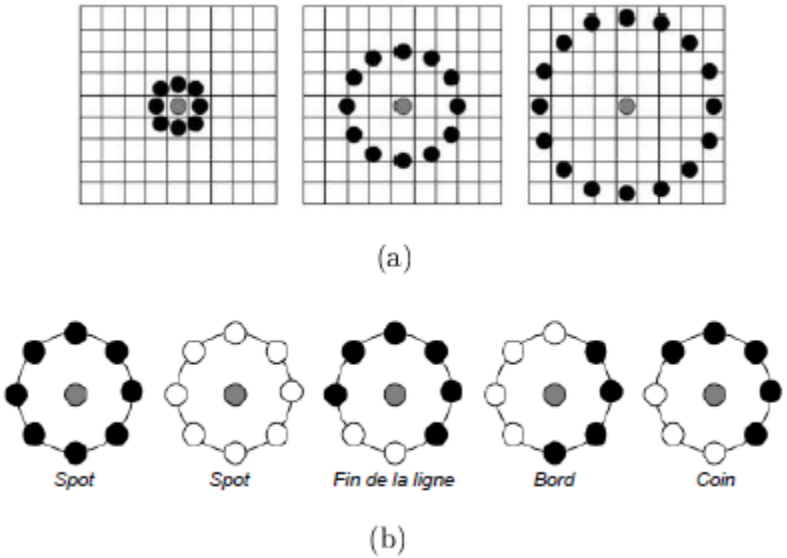


Figure 29:: Trois voisinages pour des R et P différents, (b) : Textures particulières détectées par LBPu2.

3.7.3. LBP invariant par rotation

L'invariance en rotation des motifs est obtenue en mettant les motifs similaires à une rotation prés dans un même label, diminuant encore la taille du vecteur de description à P + 2 dimensions. La figure 29 montre les neufs labels uniformes 2 et invariants en rotations obtenus dans le cas d'un rayon unitaire et de huit voisins. Les LBP uniformes 2 et invariants en rotation peuvent être définis comme :

$$LBP_{P,R}^{riu2} = \begin{cases} \sum_{p=0}^{P-1} s\left(I_R(p) - I(c)\right) & si \quad U\left(LBP_{P,R}\right) \leq 2 \\ P+1 & sinon \end{cases}$$

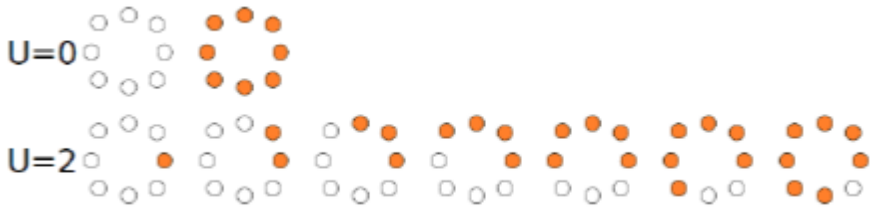


Figure 30:Motifs binaires locaux uniformes 2 et invariants en rotation.

Il est également possible de définir des motifs invariants par rotation sans utiliser de motifs uniformes, ils sont définis comme :

$$LBP_{P,R}{}^{ri} = min\{ ROR(LBP_{P,R}, i) \quad | i = 0,1, \dots, P-1$$

Où l'opérateur ROR (x, i) effectue une permutation circulaire du nombre binaire x, ayant une longueur de P bits, i fois vers la droite, avec i < |P|.

Néanmoins, cette invariance en rotation est à prendre au niveau des motifs et non de l'image. En effet, elle ne prend pas en compte les artefacts issus de l'échantillonnage ni les variations de textures causées par les modifications des sources d'illumination.

La figure 30 illustre les 36 modèles binaires locaux invariants en rotation uniques pouvant se produire. Dans le cas de P = 8, c'est-à-dire $LBP_{8,R}{}^{ri}$ peut avoir 36 valeurs différentes. Par exemple, le motif n° 0 détecte des points lumineux, points noirs le n°8 et zones plates, et bords le n° 4.

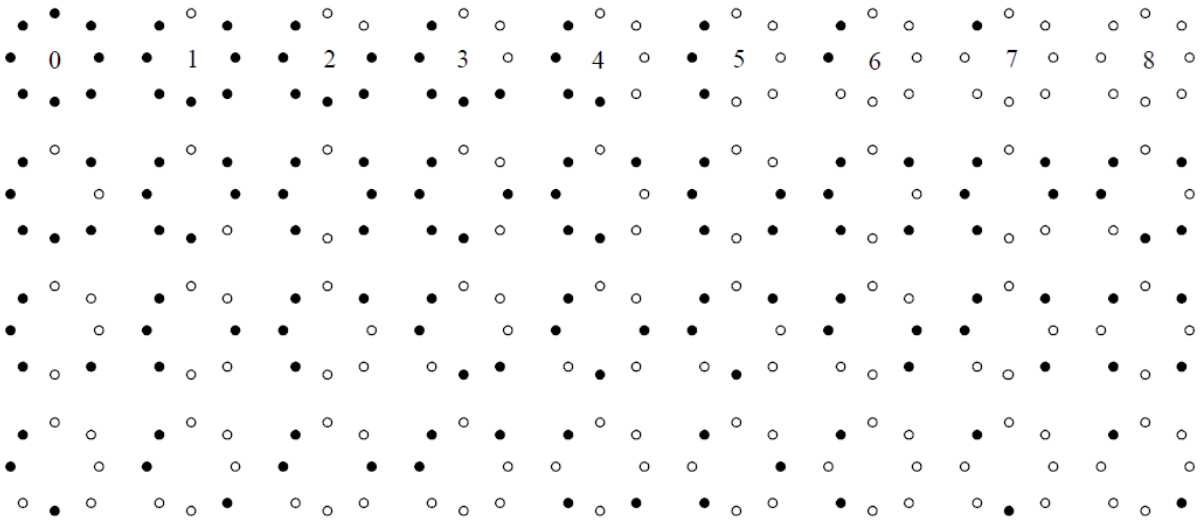


Figure 31:Les 36 modèles binaires uniques invariants en rotation qui peuvent apparaître

Dans le cercle symétrique ensemble voisin de $LBP_{8,R}{}^{ri}$. Les cercles noir et blanc correspondent aux valeurs de bits 0 et 1 dans la sortie 8 bits de l'opérateur. La première rangée contient les neuf modèles « uniformes » et les nombre sà l'intérieur correspondent à leur unique $LBP_{8,R}{}^{riu2}$ codes.

3.2.5.3 Histogramme

Souvent la distribution des codes LBP sur l'image est utilisée pour décrire la texture sous forme d'histogramme.

Une fois le code LBP est calculé pour tous les pixels de l'image, on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image.

En réalité, afin d'incorporer plus d'informations spatiales au vecteur représentant l'image (par exemple le visage), on divise tout d'abord cette image codée par l'opérateur LBP en petites régions et l'histogramme sera construit pour chaque région. Finalement, on concatène tous les histogrammes des régions afin de former un grand histogramme représentant l'image des caractéristiques faciales (voir la figure ci-après). L'efficacité du code LBP comme indice facial s'explique par le fait que le LBP permet de caractériser les détails fins d'un visage

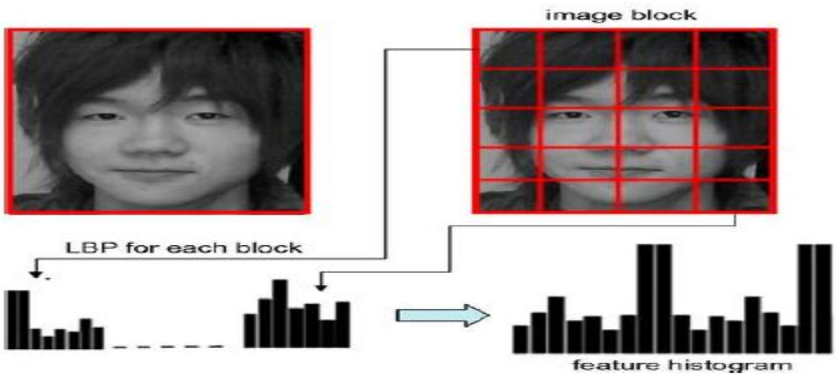


Figure 32:Exemple d'un histogramme LBP d'une image faciale.

L'histogramme LBP est connu sous cette forme :

Équation 19:formule de l'histogramme LBP

$$\boldsymbol{h(i)} = \sum_{x,y} B(LBP(x,y) = i)$$

$$\text{Avec : } i \in [0, \dots, 2^p - 1] \qquad \text{et} \qquad B(v) = \begin{cases} 1, & lorsque\ v\ est\ vraie \\ 0, & autrement \end{cases}$$

3.2.5.4 Extraction de caractéristiques par LBP

L'algorithme ci-dessous montre comment les caractéristiques de l'image de l'email sont extraites en utilisant la méthode LBP.

Algorithme 1: Extraction de caractéristiques de l'image à l'aide de LBP

Entrée : Image de l'e-mail (I)

Sortie : Vecteur de caractéristiques *LBP_FeatureVector*

Début

1. Lisez l'image de l'e-mail (I)
2. Convertissez l'image de l'e-mail (I) en image en niveaux de gris (G).
3. Divisez G en blocs (chaque bloc 3x3 pixels).
4. Pour chaque pixel d'un bloc,

4.1 Comparez-le avec ses voisins de 8 pixels (en haut à gauche, au milieu à gauche, en bas à gauche, en haut à droite, etc.).

4.2 Comparez-le avec les pixels le long d'un cercle, c'est-à-dire dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre.

4.3 Comparez-le avec le centre. Si la valeur du pixel est supérieure à la valeur du voisin, écrivez "0" Sinon, écrivez "1".

5. Enregistrez le résultat de l'étape (4) qui est le nombre binaire à 8 chiffres en *binaireim*.
6. Convertissez *binaryim* en nombre décimal en utilisant "équation décrite en haut" pour obtenir un motif binaire local (LBP)
7. Calculez l'histogramme pour chaque nombre dans LBP, pour obtenir un vecteur de caractéristiques à 256 dimensions.
8. Normalisez l'histogramme et enregistrez-le dans *LBP_FeatureVector*.
9. Retournez le vecteur de caractéristique LBP

Fin.

3.2.6 Combinaison des caractéristiques

À cette étape, les caractéristiques extraites par les différentes méthodes sont combinées pour former un seul vecteur de caractéristiques combiné en tant qu'entrées dans le classificateur pour décider si l'image testée est de type spam ou non spam.

Le LBP (Local Binary Pattern) et le GLCM (Gray-Level Co-occurrence Matrix) sont deux techniques de traitement d'images très utilisées pour extraire les caractéristiques des images. La combinaison de ces deux techniques peut fournir des informations plus riches et plus complètes sur les images. Il existe plusieurs méthodes pour combiner les vecteurs de caractéristiques LBP et GLCM. Voici quelques-unes des méthodes les plus courantes :

1. **Concaténation** : Dans cette méthode, les vecteurs de caractéristiques LBP et GLCM sont simplement concaténés pour former un vecteur de caractéristiques combiné. Cette méthode est simple et facile à implémenter, mais elle peut entraîner des problèmes de dimensionnalité et peut ne pas être suffisamment efficace pour représenter toutes les informations pertinentes de l'image.
2. **Fusion pondérée** : Cette méthode consiste à attribuer un poids à chaque vecteur de caractéristiques avant de les combiner. Les poids peuvent être déterminés soit manuellement en fonction de l'importance relative des deux caractéristiques, soit automatiquement à l'aide d'un algorithme d'apprentissage automatique. Cette méthode est plus flexible que la concaténation, mais elle nécessite une sélection soigneuse des poids pour obtenir les meilleurs résultats.
3. **PCA (Principal Component Analysis)** : Dans cette méthode, les vecteurs de caractéristiques LBP et GLCM sont projetés dans un espace latent de dimensions plus faibles à l'aide de l'analyse en composantes principales (PCA), puis les composantes principales sont combinées pour former un vecteur de caractéristiques combiné. Cette méthode permet de réduire la dimensionnalité et d'éviter les problèmes de surapprentissage, mais elle peut perdre certaines informations importantes de l'image.
4. **SVM (Support Vector Machine) :** Cette méthode utilise un SVM pour classifier les images en utilisant à la fois les vecteurs de caractéristiques LBP et GLCM. L'approche consiste à entraîner un classificateur SVM sur les deux types de caractéristiques, puis à utiliser les sorties du classificateur pour fusionner les caractéristiques. Cette méthode peut donner de bons résultats de classification, mais elle peut être plus coûteuse en temps de calcul.

Il n'y a pas de méthode de combinaison de caractéristiques universelle pour toutes les tâches de traitement d'images. Le choix de la méthode dépend de la nature de la tâche et des données disponibles. Il est donc important d'évaluer différentes méthodes et de choisir celle qui convient le mieux à votre problème spécifique.

3.2.7 Classification

Dans notre travail, l'objectif principal de la classification des spams est de faire la distinction entre le spam et l'image légitime ou utile (Ham). Les classificateurs classent les images en deux classes "Ham" ou "Spam" en comparant les caractéristiques extraites des images avec l'une d'un ensemble donné de classes. Une fois l'image identifiée et classée grâce à ses caractéristiques, celles-ci sont ensuite enregistrées comme modèles pour les classes formées. Pour la classification des spams, de nombreux algorithmes d'apprentissage ont été utilisés, tels que : Machine à Vecteur de support

(SVM), et K Plus Proche Voisin (KNN). L'objectif principal est de sélectionner le meilleur algorithme pour classifier les images spams.

3.2.7.2 K voisins les plus proches

La méthode K voisins les plus proches (KNN) a prouvé son efficacité face au traitement des données textuelles. La phase d'apprentissage consiste à stocker les exemples étiquetés. Le classement de nouveaux textes s'opère en calculant la similarité entre la représentation vectorielle du document et celle de chaque exemple du corpus d'apprentissage. Les k éléments les plus proches sont sélectionnés et le document est assigné à la classe majoritaire (le poids de chaque exemple dans le vote étant éventuellement pondéré par sa distance).

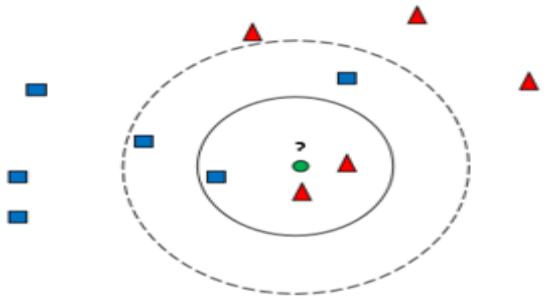


Figure 33:K voisins les plus proches

Le choix de la valeur de k est dépendant de la taille de l'échantillon et des classes, et influence les résultats de la classification. Dans l'exemple de la Figure 32, l'objet rond sera classifié triangle si k=3 et classifié Carré si k=5.

Lorsque « k » est petit, la classification est plus sensible à cause des documents appartenant à une classe mais dont leur vecteur de représentation ressemble beaucoup plus à une autre. Par contre, lorsque « k » est trop grand, les catégories ayant peu d'exemples peuvent être désavantagées par rapport à celles qui en ont plus. On peut remédier à cela en pondérant le vote par la distance qui sépare les plus proches voisins de l'individu à classer.

Si la qualité de catégorisation obtenue par les k plus proches voisins (KNN) est satisfaisante que celle obtenue avec d'autres méthodes qui nécessitent un apprentissage complexe, le temps nécessaire à son déroulement peut être un obstacle difficilement incontournable ; là où la complexité des autres méthodes est fonction du nombre de catégories.

3.2.7.3 Machines à support vectoriels (SVM)

Une machine à vecteur de support (SVM) est un algorithme d'apprentissage automatique supervisé qui est principalement utilisé pour la classification. Un SVM tente de trouver un hyperplan, qui sépare les échantillons dans l'ensemble de données. Le but de SVM est de trouver un classificateur qui sépare au mieux les données et maximise la distance entre ces deux classes. En d'autres termes, parmi tous les hyperplans possibles qui peuvent séparer les échantillons, le SVM trouve celui qui a la distance maximale de tous les points.

Les points les plus proches, qui seuls sont utilisés pour la détermination d'hyperplan, sont appelés vecteurs de support.

De plus, les SVM traitent aussi des données qui ne sont pas linéairement séparables. Pour cela, il existe deux méthodes : l'introduction de marges souples ou l'utilisation de l'astuce du noyau.

- Les marges souples fonctionnent en autorisant quelques éléments mal classés tout en conservant la capacité de prédiction la plus élevée de l'algorithme. En pratique, il est préférable de ne pas surapprendre le modèle d'apprentissage de la machine, et nous pourrions le faire en assouplissant certaines des hypothèses de la machine à vecteur de support.
- L'astuce du noyau résout le même problème d'une manière différente. Imaginons que nous ayons un espace à deux dimensions, mais que les classes soient linéairement inséparables. L'astuce du noyau utilise une fonction noyau qui transforme les données en y ajoutant d'autres dimensions.

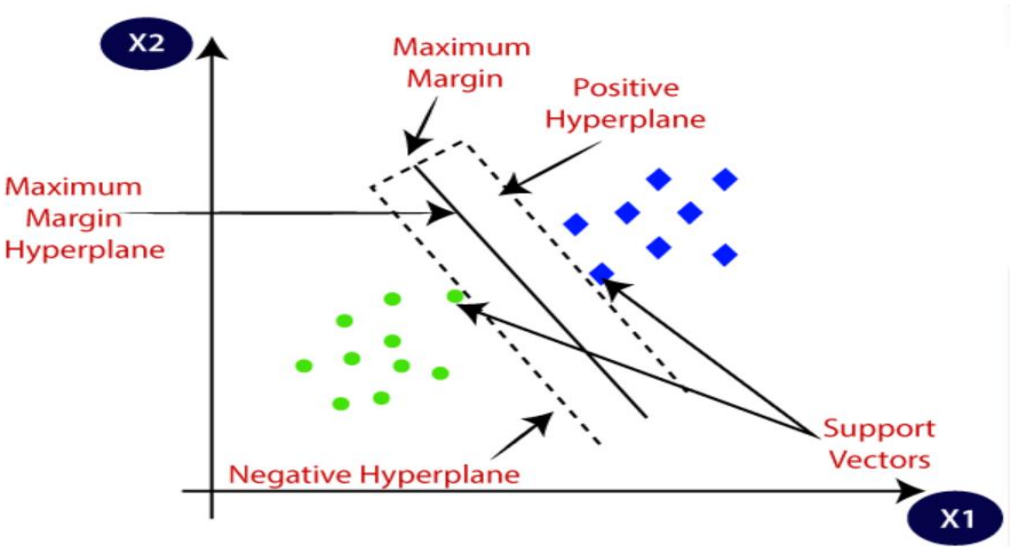


Figure 34:Machines à support vectoriels (SVM)

Remarques sur les algorithmes d'apprentissage supervisé (KNN ; SVM) :

1. **Les SVM** donnent de très bons résultats de classification de textes mais sont très coûteux en temps d'apprentissage et possèdent une limitation théorique, Le modèle sous-jacent à se classifier a été conçu pour la classification binaire : il cherche un plan séparateur qui sépare l'ensemble des objets en deux classes.
2. **Les KNN** sont très simples à mettre en œuvre, et permettent une implémentation rapide pour fournir des résultats satisfaisants. Cette méthode reste robuste sur des cas de données incomplètes, mais elle est très couteuse en temps de classification et stockage mémoire.

3.3 Conclusion

Dans ce chapitre se concentre sur la conception générale du système. Il présente une architecture détaillée, en commençant par l'ensemble de données utilisé. Ensuite, il décrit les différentes étapes de traitement, notamment le prétraitement des images pour améliorer leur qualité. Ensuite, deux méthodes d'extraction des caractéristiques sont abordées : la Matrice de cooccurrence des niveaux

de gris, qui permet de capturer des informations sur les textures des images, et la méthode des motifs binaires locaux (LBP), qui est sensible aux variations locales d'intensité. Les caractéristiques extraites sont ensuite combinées pour former un vecteur complet, qui est utilisé pour la classification des images. Le chapitre conclut en soulignant l'importance de ces choix de conception et en préparant le terrain pour le prochain chapitre qui traitera de la mise en œuvre du système.

Chapitre 4 : implémentation et expérimentation

4.1 Introduction

L'objectif de ce chapitre est de présenter les étapes de l'implémentation de l'approche proposée dans le cadre d'un système de détection de spam image et les différentes étapes de sa réalisation.

Nous commençons tout d'abord par la présentation des ressources, du langage et de l'environnement de développement que nous avons utilisé. Puis les étapes de la réalisation du modèle.

Nous poursuivons ce chapitre par la présentation des différents résultats expérimentaux obtenus et discussion, quelques captures d'écrans de notre application.

4.2 Outils d'implémentation

Pour implémenter et optimiser notre model, nous avons maintenant des Frameworks de DL open source faciles à utiliser qui a l'objectif de Simplifier la mise en œuvre des modèles complexes et à grande échelle.

- **Python :** Le langage de programmation scientifique multi-paradigme Python a été créé en 1989 par Guido van Rossum, aux Pays-Bas. Le nom Python vient d'un hommage à la série télévisée Monty Python's Flying Circus dont G. van Rossum est fan. La première version publique de ce langage a été publiée en 1991. Ce langage de programmation présente de nombreuses caractéristiques intéressantes :

- Il est gratuit et multiplateforme. : Windows, Mac OS X, Linux, Android, iso, depuis les mini-ordinateurs Raspberry Pi jusqu'aux supercalculateurs.
- C'est un langage de haut niveau. Il demande relativement peu de connaissance sur le fonctionnement d'un ordinateur pour être utilisé.
- C'est un langage interprété. Un script Python n'a pas besoin d'être compilé pour être exécuté, contrairement à des langages comme le C ou le C++.
- C'est un langage dynamique, extensible Il favorise la programmation structurée fonctionnelle et orientée objet. C'est-à-dire qu'il est possible de concevoir en Python des entités qui miment celles du monde réel (une cellule, une protéine, un atome, etc.) avec un certain nombre de règles de fonctionnement et d'interactions. Il est relativement simple à prendre en main (Poulain, 2019). La syntaxe de Python est très simple et, combinée à des types de données évolués (listes, dictionnaires,...), conduit à des programmes à la fois très compacts et très lisibles. Il gère ses ressources (mémoire, descripteurs de fichiers...) sans intervention du programmeur (python).
- Enfin, il est très utilisé en bioinformatique et l'intelligence artificielle et plus généralement en analyse de données. Toutes ces caractéristiques font que Python est outils idéal pour implémenter notre application.

- **PILLOW :** Pillow est une bibliothèque de traitement d'image, qui est un fork et successeur du projet PIL (Python Imaging Library). Elle est conçue de manière à offrir un accès rapide aux données contenues dans une image, et offre un support pour différents formats de fichiers tels que PPM, PNG, JPEG, GIF, TIFF et BMP.
  Pillow dispose de capacités de traitement d'images relativement puissantes, et a pour but d'offrir une solide base à toute application générale de traitement d'images.

- **OpenCV :** OpenCV (Open Source Computer Vision Library) est une bibliothèque qui aide à la vision par ordinateur Depuis son lancement officiel en 1999 par l'équipe d'Intel, un certain

nombre de programmeurs ont contribué aux derniers développements de la bibliothèque. Le dernier changement majeur intervenu en 2009 (OpenCV 2) qui inclut les principales modifications apportées à l'interface C. OpenCv est spécialisé en :

- Manipulation des données d'images et vidéo, les matrices et les vecteurs.
- Différentes structures de données dynamiques (listes, files d'attente, ensembles, arbres, graphiques).
- Analyse du mouvement (flux optique, segmentation du mouvement, suivi), Reconnaissance d'objets.
- Interface graphique de base (image / vidéo à afficher, gestion du clavier et de la souris, barres de défilement…)(Agam, 2006).

- **NumPy :** NumPy est le paquet fondamental du calcul scientifique avec Python. Il contient entre autres des choses :
  - un puissant objet tableau à N dimensions
  - fonctions sophistiquées (diffusion)
  - des outils pour l'intégration du code C / C ++ et Fortran
  - capacités utiles d'algèbre linéaire, de transformée de Fourier et de nombres aléatoires

- **Matplotlib :** Est une bibliothèque de traçage pour le langage de programmation Python et son extension mathématique numérique NumPy. Il fournit une API orientée objet permettant d'incorporer des graphiques dans des applications à l'aide de kits d'outils d'interface graphique à usage général tels que Tkinter, wxPython, Qt ou GTK +.

- **Scikit-learn :** Scikit-learn est une bibliothèque libre Python dédiée à l'apprentissage automatique. Elle est développée par de nombreux contributeurs notamment dans le monde académique par des instituts français d'enseignement supérieur et de recherche comme Inria et Télécom ParisTech. Elle comprend notamment des fonctions pour estimer des forêts aléatoires, des régressions logistiques, des algorithmes de classification, et les machines à vecteurs de support.

4.3 Environnement d'implémentation

- Processeur : Intel(R) Core(TM) i7-4700MQ CPU @ 2.40GHz 2.40 GHz
- RAM : 8,00 Go
- Système d'exploitation : Windows 10, 64 bits

4.4 Ensemble de données

Ce projet utilise la combinaison de trois ensembles de données différents :

- **Dredze Image Spam Dataset :**(Dredze et al. 2007) ont créé un ensemble de données contient 3 ensembles d'images. Ham personnel (PHam) contient 2 021 images dont 1 517 sont uniques. Personal Spam (PSpam) contient 3 298 images, dont 1 274 sont uniques. Enfin, les archives de spam (SpamArch) contiennent 16 028 fichiers de différents formats (JPEG, PNG, GIF, etc.), dont 3 039 images uniques. En outre, l'archive de spam contenait beaucoup de fichiers non traités dans différents formats tels que gif, txt, jpg, etc

- **Image Spam Hunter (ISH)** (Gao et al. 2008) : Ce dataset contient à la fois des images spam et ham au format JPEG qui sont collectées à partir des e-mails originaux. Il y a 810 images ham et

929 images spam au total. Le nombre d'images uniques de spam et de ham est de 879 et 810 respectivement.

- **Improved Dataset** (Annadatha, 2019) : Ce dataset a été créé par Aneri et al, en effectuant une transformation sur les images ham pour les faire ressembler à des spam. Les images ham ont été redimensionnées à la taille des images spam pour aligner leurs caractéristiques de métadonnées. Du bruit a été introduite dans les images spam pour rendre difficile la détection des bords, puisque les images spam ont généralement moins de bruit que les images ham. Le nombre d'images uniques dans ce jeu de données est de 975. Il est disponible à l'adresse.

Nous avons également prétraité et combiné ces ensembles de données pour en construire un seul ensemble de données. Ensuite, les expériences ont été réalisées sur cet ensemble de données.

4.5 Implémentation et Réalisation

Cette section décrit les différents modules du notre système de détection de spam image.

Notre système de détection de spam image est constitué de trois modules principaux indépendants :

4.5.1 Le module de prétraitement

En général, l'étape de prétraitement comprend les opérations suivantes.

- Unifiez les différents formats d'image en JPEG, car c'est l'un des formats d'image les plus populaires et les plus efficaces.
- Redimensionnez toutes les images à la même taille (par exemple 65 × 65).
- Convertir des images colorées en une image en niveaux de gris
- Normalisation

4.5.2 Le module d'extraction des caractéristiques

L'extraction de caractéristiques est l'une des phases les plus importantes de notre système, qui vise à extraire les propriétés caractéristiques d'une image et à les exprimer sous forme de vecteur de caractéristiques (f0,f1,f2,…,fn). La représentation qui en résultera servira de base à l'étape suivante, qui est la classification. Dans notre travail, nous nous intéressons aux méthodes d'extraction de caractéristiques de texture, plus précisément nous choisissons aux méthodes :

- La matrice de cooccurrence de niveaux de gris (GLCM)
- le modèle binaire local (LBP)

4.5.3 Le module de classification

Pour la classification de spam image, de nombreux algorithmes d'apprentissage automatique sont utilisés, tels que : Machine à Vecteur de support (SVM), K Plus Proche Voisin (KNN). L'objectif principal est de sélectionner le meilleur algorithme pour classifier les images spams.

4.6 Résultats obtenus et discussions

Après l'étape d'apprentissage, nous passons à l'étape de test afin de valider notre modèle et de voir l'intérêt de cette approche et ses avantages. Nous réalisons une série d'expérimentations pour

vérifier la faisabilité et l'efficacité de notre modèle hybride de détection de spam image qui est capable de faire la distinction entre les images spam et les images légitimes (ham) en se basant sur les caractéristiques de texture extraites de l'image.

De chaque image, deux types de caractéristiques sont extraits. La première méthode extrait les caractéristiques de texture de la matrice de cooccurrence des niveaux de gris (GLCM), tandis que la seconde méthode d'extraction de caractéristiques est le modèle binaire local (LBP) avec extraction directe des caractéristiques de texture d'image. Les caractéristiques extraites sont utilisées dans un style individuel et combiné afin d'apprendre les classifieurs au stade de la formation. Ensuite, pour classer les images en tant que spam ou ham, nous réalisons une étude comparative se basant sur deux algorithmes d'apprentissage : Machine à Vecteur de support (SVM), et K Plus Proche Voisin (KNN). L'objectif principal est de sélectionner le meilleur algorithme pour classifier l'email reçu. Chaque classifieur a été utilisé de trois manières, avec les caractéristiques de texture de l'image extraites par la méthode GLCM, puis par la méthode LBP et enfin par la fusion de ces deux caractéristiques respectivement.

Pour la validation des performances de notre modèle, nous utilisons la méthode 70/30 telle que 70% utilisée pour la phase d'apprentissage et 30% pour la phase de test.

Les mesures de performance utilisées sont la précision, le rappel et l'échelle F1 dont leurs bases de calcul se fait par rapport au tableau 2.

		Réel	
		Positive	Négative
Prédite	Positive	VP	FP
	Négative	FN	VN

Tableau 2: Tableau de confusion

Sachant que :

- Vrai positif (VP) : indique le nombre d'images spam correctement classées comme des images spam.
- Faux positif (FP) : indique le nombre d'images ham (non-spam) classées à tort comme des images spam.
- Vrai négatif (VN) : indique le nombre d'images ham (non-spam) correctement classées comme des images ham
- Faux négatif (FN) : indique le nombre d'images spam classés à tort comme des images ham.

Tel que les métriques que nous avons étudiées sont présentées sous les formes suivantes :

- $Accuracy = \frac{VP+VN}{VP+VN+FP+FN}$
- $Precision = \frac{VP}{VP+FP}$

- $Rappel = \frac{VP}{VP+FN}$
- $F1\_mesure = 2 \times \frac{Precision \times Rappel}{Precision+Rappel}$

Avant d'effectuer les différents tests, nous avons procédé à la paramétrisation des différentes méthodes d'extraction de caractéristiques, à savoir LBP (Local Binary Patterns), GLCM (Grey-Level Co-occurrence Matrix) et LBP+GLCM, ainsi que des paramètres des classifieurs SVM (Support Vector Machine) et KNN (K-Nearest Neighbors).

Pour la méthode GLCM, plusieurs paramètres sont pris en compte pour garantir une extraction précise des caractéristiques. Parmi ces paramètres, nous avons ajusté la distance de séparation entre les pixels voisins d = [1, 2, 3] et l'orientation des textures à considérer θ = (0°,45°,90°,135°), ainsi que le nombre de niveaux de gris à utiliser dans la construction de la matrice de co-occurrence. Pour le calcul des caractéristiques basées sur le GLCM, il est donc essentiel de normaliser la matrice GLCM pour obtenir une sorte de matrice de probabilité. De la matrice de co-occurrence de niveau de gris nous avons extraits différentes caractéristiques tels que : contrast, dissimilarity, homogeneity, energy, correlation, etc.

Pour la méthode LBP, plusieurs paramètres sont pris en compte lors de la phase de paramétrisation. Nous avons ajusté des aspects tels que la taille de la fenêtre, le rayon de voisinage (R=1) et le nombre de points (n=8) pour assurer une extraction adéquate des caractéristiques des images.

Concernant les classifieurs SVM et KNN, nous avons ajusté leurs paramètres respectifs pour optimiser leurs performances de classification. Ces paramètres incluent des éléments tels que le noyau utilisé (linear, poly, rbf et sigmoid), le coût d'erreur (C=1), le paramètre K (K=5), etc. La sélection et l'ajustement judicieux de ces paramètres permettent d'obtenir des résultats plus précis et fiables lors de la phase de classification.

En effectuant cette étape de paramétrisation préliminaire, nous nous assurons d'exploiter au mieux les méthodes d'extraction de caractéristiques et les classifieurs, afin d'obtenir des résultats de classification plus précis et efficaces dans notre système de détection de spam image.

À partir des images spam et ham des differentes dataset, nous avons extrait 60 caractéristiques par la méthode GLCM, 256 caractéristiques par la méthode LBP et 316 par la méthode hybride.

4.6.1 Dataset1 (dredze)

Nous avons utilisé 70 % des images ham et spam comme ensemble d'entraînement et 30% pour les tests. Au total, 878 images spam et 976 images ham ont été utilisées pour l'entrainement. Les 377 images spam et 417 images ham restantes ont été utilisées pour les tests.

Les figures 35, 36 et 37 montrent les matrices de confusion pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

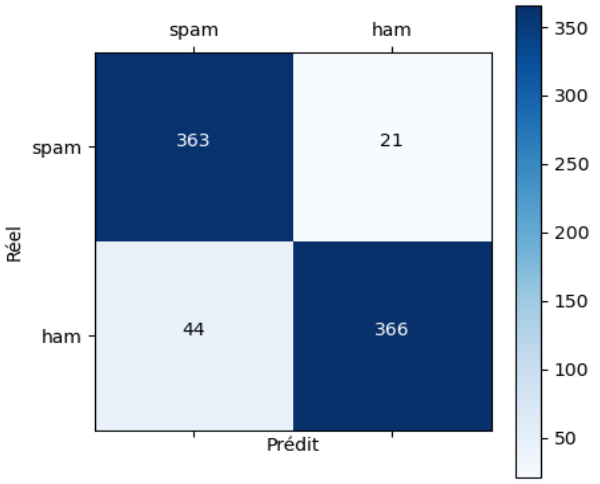


Figure 35:matrice de confusion (GLCM + SVM)

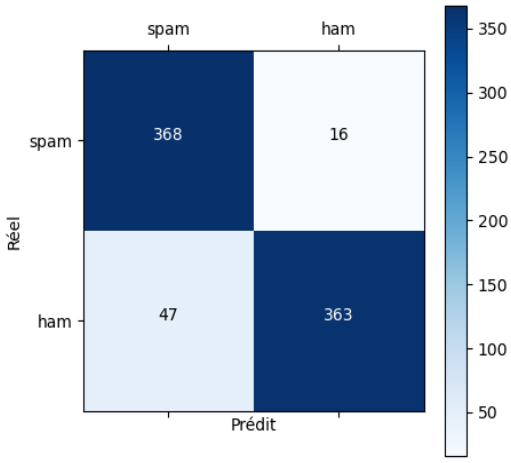


Figure 36:matrice de confusion (LBP + SVM)

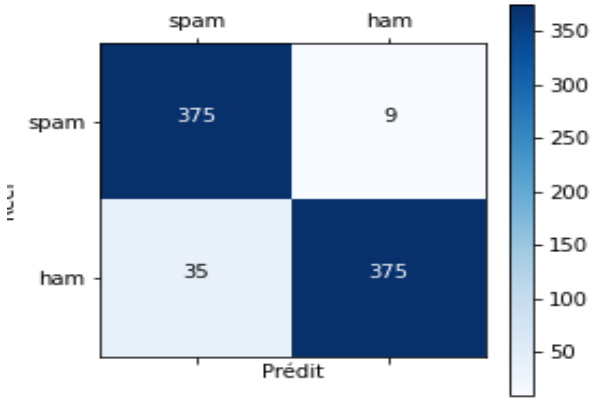


Figure 37:matrice de confusion (GLCM-LBP + SVM)

Les figures 38, 39 et 40 montrent les courbes ROC pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

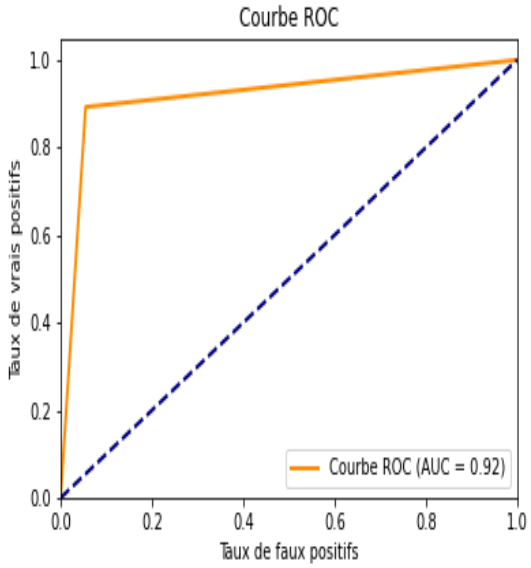


Figure 38:Courbe ROC (GLCM + SVM)

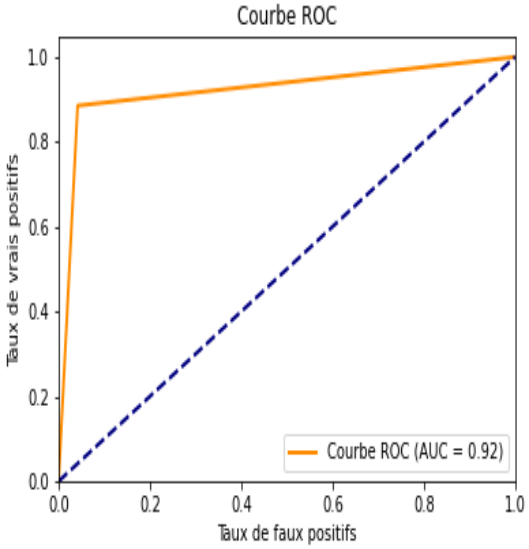


Figure 39:Courbe ROC (LBP + SVM)

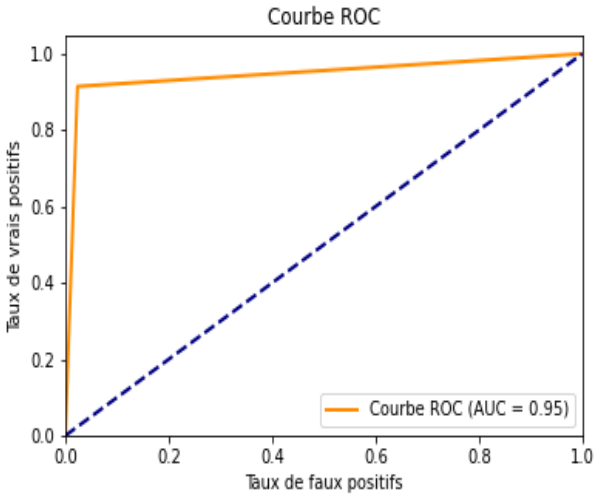


Figure 40:Courbe ROC (GLCM-LBP + SVM)

Le tableau 3 résume le rapport de classification pour le dataset1.

Modele	SVM				KNN			
	Prec.	Rappel	F1	Acuracy	Prec.	Rappel	F1	Acuracy
LBP	92,00	92,00	92,00	92,07	94,00	94,00	94,00	93,70
GLCM	92,00	92,00	92,00	91,81	93,00	93,00	93,00	92,70
LBP+GLCM	95,00	95,00	94,00	94,46	95,00	95,00	95,00	95,34

Tableau 3 : Résultat de classification - dataset1

4.6.2 Dataset2 (IHS)

Nous avons utilisé 70 % des images ham et spam comme ensemble d'entraînement et 30% pour les tests. Au total, 615 images spam et 565 images ham ont été utilisées pour l'entrainement. Les 267 images spam et 242 images ham restantes ont été utilisées pour les tests.

Les figures 41, 42 et 43 montrent les matrices de confusion pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

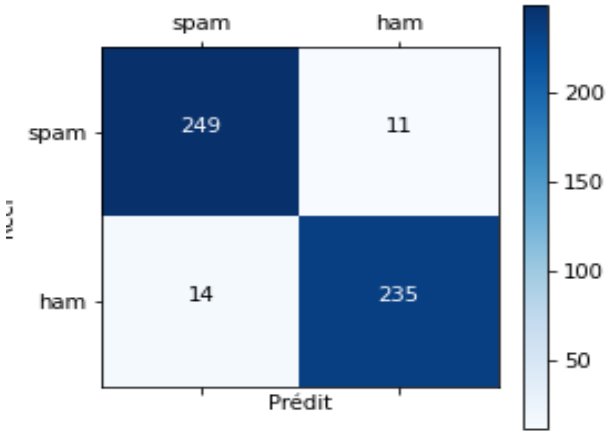


Figure 41:matrice de confusion (GLCM + SVM)

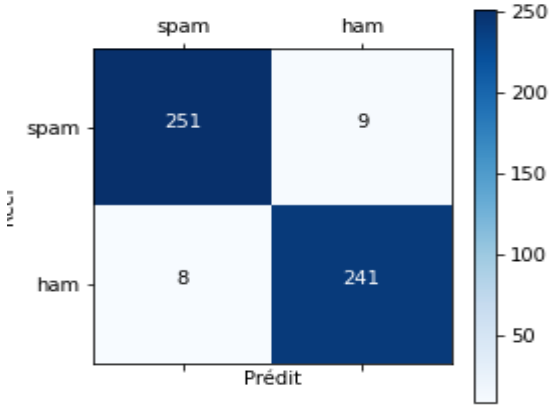


Figure 42:matrice de confusion (LBP + SVM)

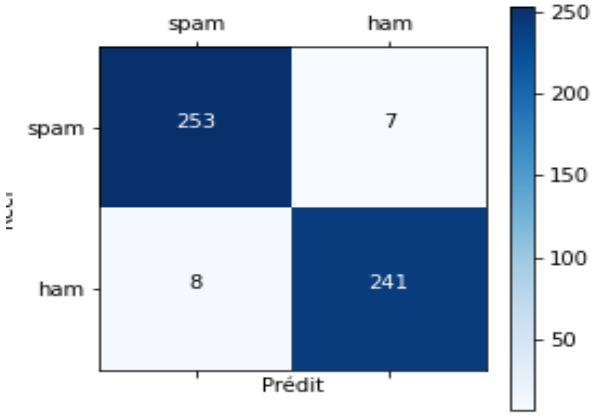


Figure 43:matrice de confusion (GLCM-LBP + SVM)

Les figures 44, 45 et 46 montrent les courbes ROC pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

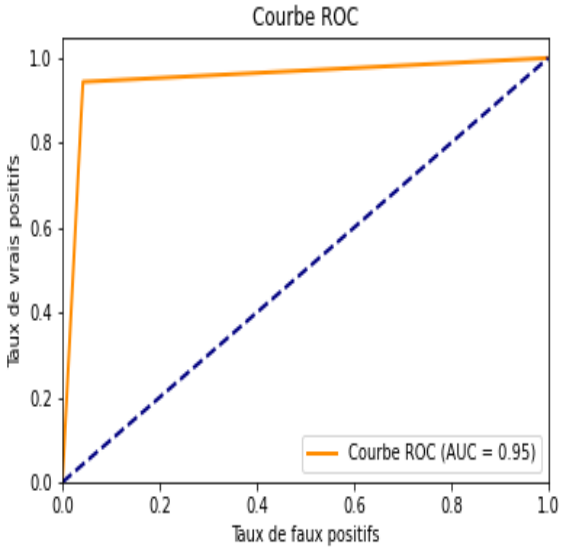


Figure 44:courbe ROC (GLCM+SVM)

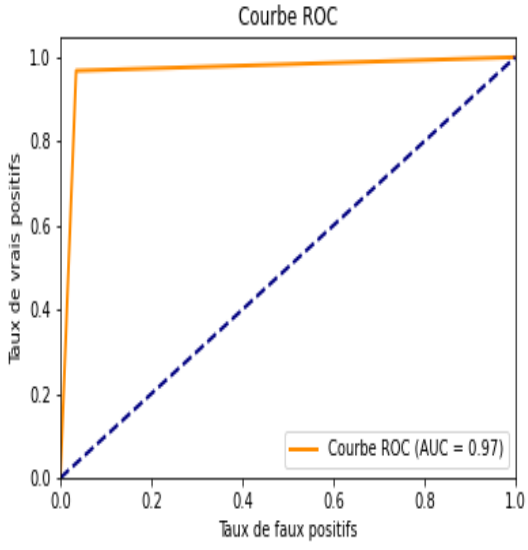


Figure 45: Courbe ROC (LBP + SVM)

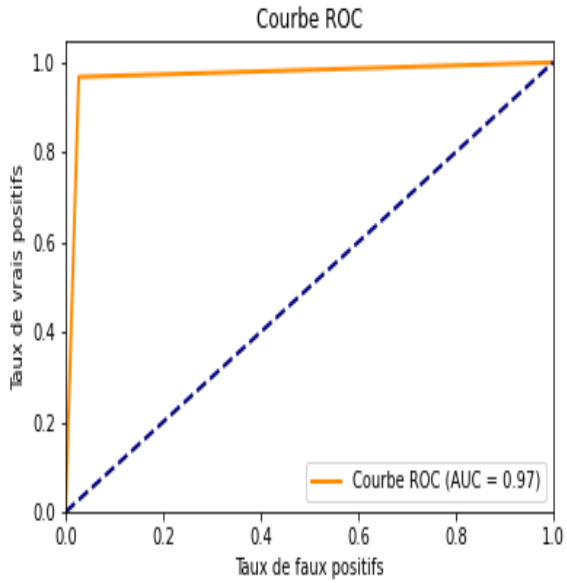


Figure 46:Courbe ROC (GLCM-LBP + SVM)

Le tableau 4 résume le rapport de classification pour le dataset2.

Modele	SVM				KNN			
	Prec.	Rappel	F1	Acuracy	Prec.	Rappel	F1	Acuracy
LBP	97,00	97,00	97,00	96,66	97,00	97,00	97,00	97,25
GLCM	95,00	95,00	95,00	95,09	95,00	95,00	95,00	95,09
LBP+GLCM	97,00	97,00	97,00	97,05	97,00	97,00	97,00	97,25

Tableau 4:Résultat de classification – dataset2

4.6.3 Dataset3 (Combine)

Nous avons utilisé 70 % des images ham et spam comme ensemble d'entraînement et 30% pour les tests. Au total, 2182 images spam et 1538 images ham ont été utilisées pour l'entrainement. Les 935 images spam et 659 images ham restantes ont été utilisées pour les tests.

Les figures 47, 48 et 49 montrent les matrices de confusion pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

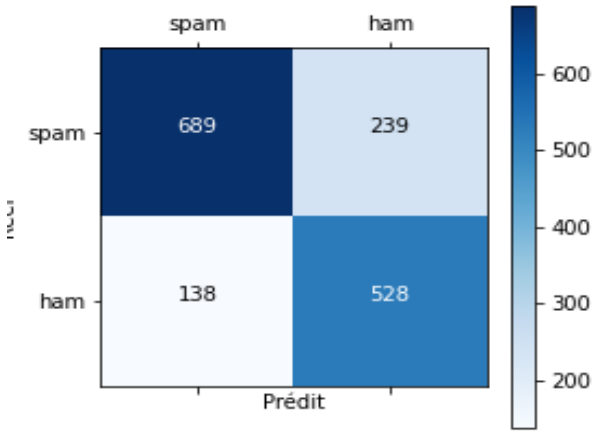


Figure 47:matrice de confusion (GLCM + SVM)

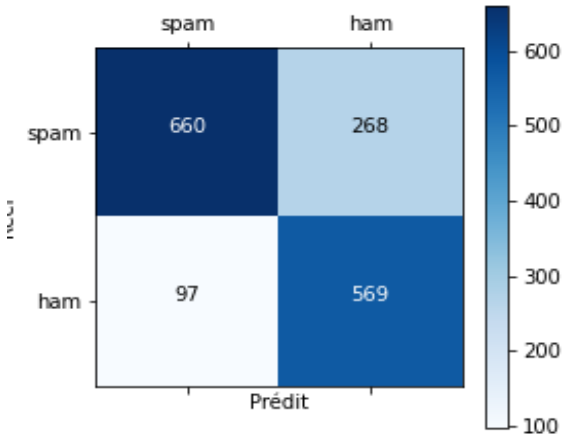


Figure 48:matrice de confusion (LBP + SVM)

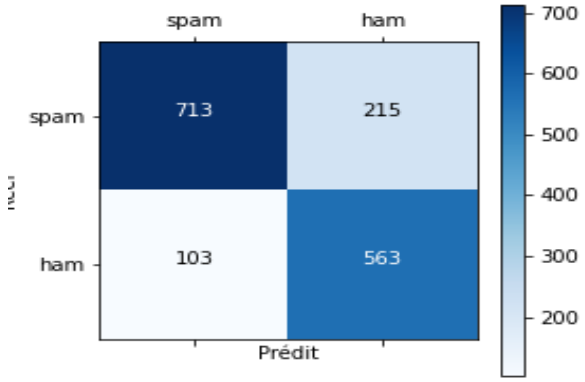


Figure 49:matrice de confusion (GLCM-LBP + SVM)

Les figures 50, 51 et 52 montrent les courbes ROC pour les trois méthodes d'extraction de caractéristiques GLCM, LBP et GLCM+LBP respectivement pour le classifieur SVM (noyau linéaire).

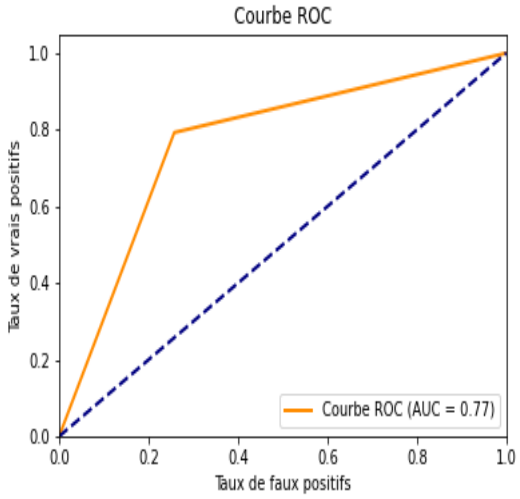


Figure 50:Courbe ROC (GLCM + SVM)

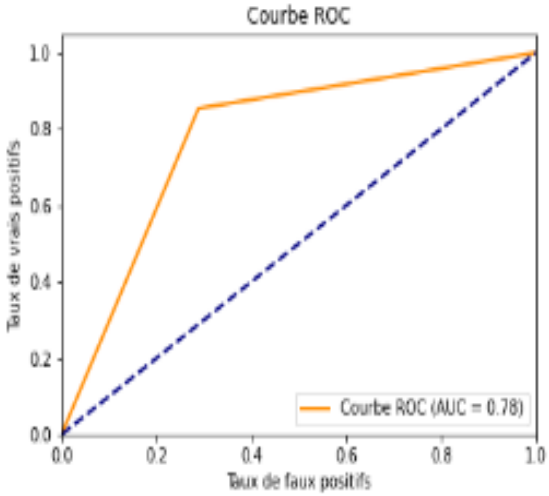


Figure 51:Courbe ROC (LBP + SVM)

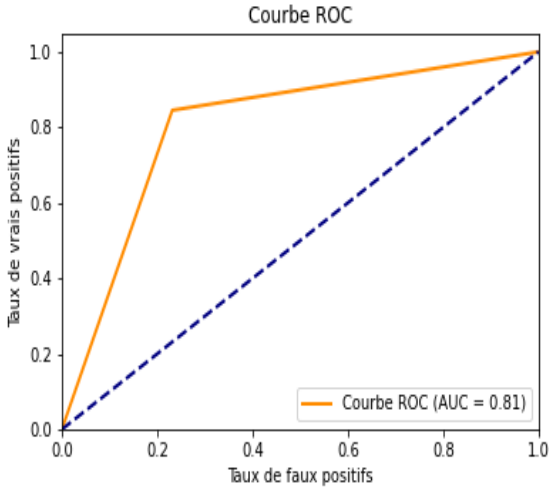


Figure 52:Courbe ROC (GLCM-LBP + SVM)

Le tableau 5 résume le rapport de classification pour le dataset3.

Modele	SVM				KNN			
	Prec.	Rappel	F1	Acuracy	Prec.	Rappel	F1	Acuracy
LBP	78,00	76,00	77,00	**77,10**	77,00	74,00	75,00	**76,47**
GLCM	76,00	77,00	76,00	**76,35**	76,00	74,00	75,00	**75,91**
LBP+GLCM	80,00	81,00	80,00	**80,05**	79,00	78,00	78,00	**79,36**

Tableau 5:Résultat de classification – dataset3

Discussions

D'après le tableau 3 qui résume les résultats de classification pour le dataset1, nous constatons que le modèle d'extraction de caractéristiques hybride GLCM+LBP donne un meilleur taux de précision (pour le SVM 94.46% et pour le KNN 95.34%) par rapport aux autres modèles (GLCM seul et LBP seul).

D'après le tableau 4 qui résume les résultats de classification pour le dataset2, nous constatons que le modèle d'extraction de caractéristiques hybride GLCM+LBP donne un meilleur taux de précision (pour le SVM 97.00% et pour le KNN 97.25%) par rapport aux autres modèles (GLCM seul et LBP seul).

D'après le tableau 5 qui résume les résultats de classification pour le dataset3, nous constatons que le modèle d'extraction de caractéristiques hybride GLCM+LBP donne un meilleur taux de précision (pour le SVM 80.05% et pour le KNN 79.36%) par rapport aux autres modèles (GLCM seul et LBP seul).

En conclusion, le modèle d'extraction de caractéristiques hybride GLCM+LBP donne de meilleurs résultats par rapport aux autres modèles (GLCM seul et LBP seul).

4.7 L'interface de l'application

La figure 53 ci-dessous montre l'interface principale de notre application de détection de spams image.

Figure 53:interface principale du système de détection de spam image

Description de l'interface principale

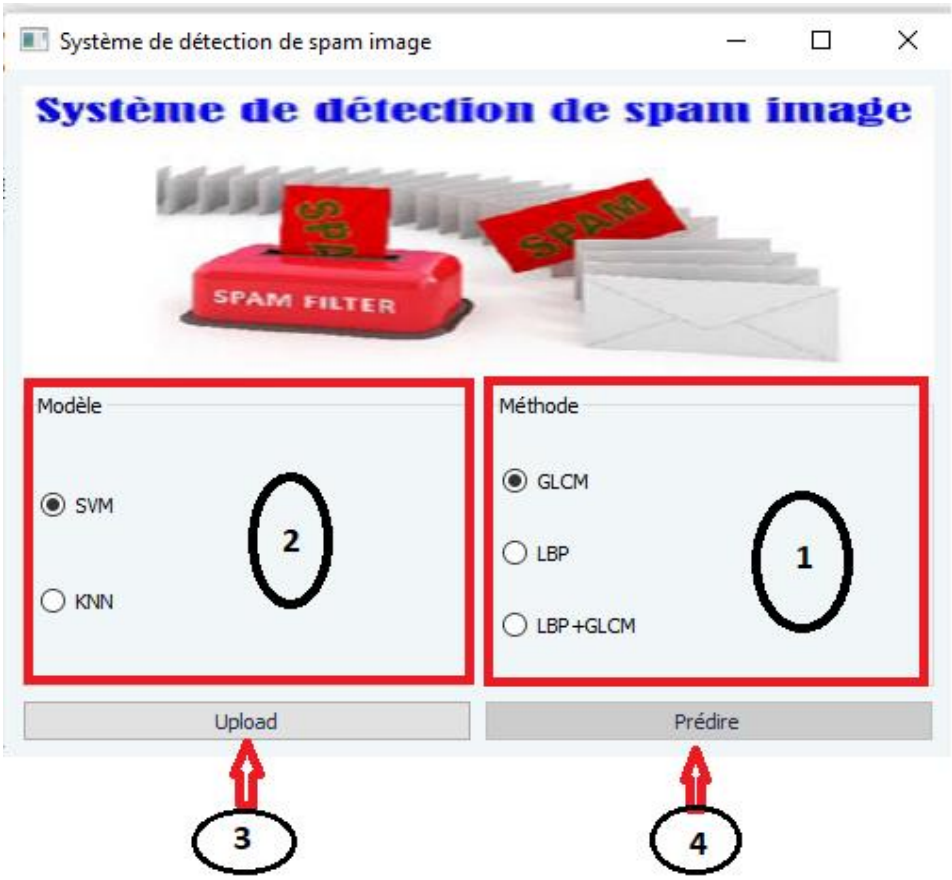


Figure 54:Description de l'interface

1- des radio-button pour choisir la méthode **GLCM, LBP ou Hybride**

2- des radio-button pour choisir le modèle **SVM ou KNN**

3-Bouton « Upload » pour charger une image.

4- Bouton « Prédire » pour prédire la classe de l'mage (Spam ou Ham)

Figure 55:l'affichage de la classe

4.8 Conclusion

Dans ce chapitre a été consacré à l'implémentation et à l'expérimentation de notre système. Les résultats obtenus sont encourageants et démontrent l'efficacité de notre approche dans la classification des données. Cependant, des perspectives d'amélioration subsistent, notamment en termes d'optimisation des performances, d'extension du système à d'autres ensembles de données et d'exploration de nouvelles techniques de classification. Pour conclure, les expérimentations ont montré que la méthode d'extraction de caractéristiques hybride (lbp+glcm) est le plus efficace par rapport aux autres méthodes (GLCM seul et LBP seul) en termes de précision.

Conclusion générale

La présente étude avait pour objectif de développer un système de détection et de filtrage de spam image en utilisant l'analyse de texture. Tout au long de ce projet, nous avons exploré différentes notions liées au spam, y compris sa définition, ses types, ses objectifs et son impact sur les utilisateurs et les fournisseurs. Ensuite, nous avons approfondi notre compréhension de l'analyse de texture, en examinant ses caractéristiques, ses types et ses méthodes d'analyse.

En se basant sur ces connaissances, nous avons conçu une architecture générale pour notre système de détection de spam image. Cette architecture comprend différentes étapes telles que la collecte de données, le prétraitement, l'extraction des caractéristiques à l'aide de la matrice de cooccurrence des niveaux de gris et de la méthode des motifs binaires locaux (LBP), la combinaison des caractéristiques extraites et la classification.

Nous avons mis en œuvre notre système en utilisant les outils appropriés et avons réalisé des expérimentations en utilisant trois ensembles de données différents : Dataset1 (dredze), Dataset2 (IHS) et Dataset3 (combine). Les résultats obtenus ont démontré l'efficacité de notre approche de détection de spam image, avec des taux de détection élevés et des performances satisfaisantes.

En conclusion, notre travail a abouti au développement d'un système de détection et de filtrage de spam image basé sur l'analyse de texture. Ce système présente des résultats prometteurs en termes de détection de spam image et peut contribuer à améliorer la sécurité et la fiabilité des communications en ligne. Cependant, il convient de noter que des améliorations supplémentaires peuvent être apportées, notamment en explorant d'autres méthodes d'analyse de texture et en utilisant des ensembles de données plus vastes.

Bibliographie

(Annadatha & Stamp, 2018): Annadatha, A., & Stamp, M. (2018). Image spam analysis and detection. Journal of Computer Virology and Hacking Techniques, 14(1), 39–52. doi:10.1007/s11416-016-0287-x.

(Anand et al., 2012): Gupta Anand, Chhavi Singhal, and Somya Aggarwal (2012). "Identification of image spam by using low level & metadata features." International Journal of Network Security & ITS Applications 4, no. 2.

(Dada et al, 2019): Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwae, O. E. (2019). Machine learning for email spam filtering: Review, approaches and open research problems.Heliyon, 5 (6), e01802.

(Dhabi et al. 2020): Dhahi E.H., Ali S.A., and Naser M.A. (2020) Text Region Extraction for Noisy Spam Image. In: Mallick P., Balas V., Bhoi A., Chae GS. (eds) Cognitive Informatics and Soft Computing. Advances in Intelligent Systems and Computing, vol 1040. Springer, Singapore.

(Dredze, et al, 2007): Dredze, M, Gevaryahu, R. & Elias-Bachrach, A., (2007). Learning fast classifiers for image spam. in CEAS, 2007, pp. 2007–487.

(Dhanaraj & Karthikeyani, 2013): Dhanaraj, S., & Karthikeyani, V. (2013). A study on e-mail image spam filtering techniques. In 2013 international conference on pattern recognition, informatics and mobile engineering (pp. 49–55).

(Gao et al., 2008): Gao, Y., Yang, M., Zhao, X., Pardo, B. Wu, Y. , Pappas, T. N. & Choudhary, A. (2008). Image spam hunter, IEEE International Conference on Acoustics, Speech and Signal Processing., pp. 1765–1768.

(Hassanet al., 2017): Hassan, M., Mirza, W., & Hussain, M. (2017, October). Header based spam filtering using machine learning approach. International Journal of Emerging Technologies in Engineering Research, 5 (10), 133–140.

Hosseini et. al (2015): Hosseini, M. S. & Rahmati, M.. (2015). A Method for Image Spam Detection Using Texture Features, International Academic Journal of Science and Engineering, vol. 2, pp. 51-58, 2015.

(Kumar, R, & KP, 2018): Kumar, A. D., R, V., & KP, S. (2018). Deep image spam: Deep learning-based image spam detection. Retrieved from https://arxiv.org/abs/1810.03977.

(Kumaresan et. al 2015): Kumaresan, T., Sanjushree, S., Suhasini, K. & Palanisamy, C. (2015). Image spam filtering using support vector machine and particle swarm optimization. IJCA Proceedings on National Conference on Information Processing and Remote Computing.

-(Liu et al. 2010): Liu Q, Zhang F, Qin Z, Wang C, Chen S, Ma Q (2010) Feature selection for image spam classification. In: International conference on communications, circuits and systems (ICCCAS), China.

(Nisha et Gaikwad, 2015): Nisha D. Chopra, K. P. Gaikwad, (2015). Image and Text Spam Mail Filtering, International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol 5, pp.15-18, June 2015.

numpy: (s.d.). Récupéré sur https://www.numpy.org/

(Poulain, 2019): Poulain, P. F.-P. (2019). livre Cours de Python. Université Sorbonne paris.

H. Jin, Q. Liu, H. Lu, and X. Tong, Face detection using improved LBP under Bayesian framework. International Conference on Image and Graphics, pp. 306-309, Hong Kong, China, 2004.

D. Huang, Y. Wang, and Y. Wang, A robust method for near infrared face recognition based on extended local binary pattern. In: G. Bebis et al. (eds) Advances in Visual Computing. ISVC 2007. Lecture Notes in Computer Science, Vol. 4842. Springer, Berlin, Heidelberg.

Z. Guo, L. Zhang, and D. Zhang, A completed modeling of local binary pattern operator for texture classification. IEEE Transactions on Image Processing, Vol. 19, No. 6, pp. 1657-1663, 2010.

R. XU, X. ZHAO, X. LI, C. KWAN et C. CHANG, « Target detection with improved image texture feature coding method and support vector machine, » International Journal of Intelligent Technology, t. 1, no 1, p. 47-56, 2006.

M. HALL-BEYER, « GLCM texture : a tutorial v. 3.0 March 2017, » 2017.

(python): python. (s.d.). Récupéré sur http://www.linux-center.org/articles/9812/python.html

(Rex Ying, 2018): Rex Ying, R. H.-c. (2018). Graph convolutional neural networks for web-scale recommender systems. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery.

(Runbox, 2017): How email works. (2017). https://blog.runbox.com/articles/how-email-works/.

(Tolentino, 2015): Tolentino, J. (2015). 5 types of social spam (and how to prevent them). TNW. https://thenextweb.com/future-of-communications/2015/04/06/5-types-of-social-spam-and-how-to-prevent-them/.

(Coroyer, 1996) : Christophe Coroyer, 1996, « Apports des corrélations d'ordre élevé à l'analyse de textures non gaussiennes » thèse de doctorat, Université Cergy-Pontoise, France.

(YANG , 2012) : X. YANG, S. TRIDANDAPANI, J. J. BEITLER, D. S. YU, E. J. YOSHIDA, W. J.CURRAN et T. LIU, « Ultrasound GLCM texture analysis of radiation-induced parotid-gland injury in head-and-neck cancer radiotherapy: An in vivo study of late toxicity, » Medical physics, t. 39, no 9, p. 5732-5739, 2012.

(Chang, 2001) : C.C. Chang, and C.J. Lin, LIBSVM: a library for support vector machines. http://www.csie.ntu.edu.tw/cjlin/libsvm, 2001.

(Zhang , 2017) : X. Zhang, J. Cui, W. Wang, and C. Lin, "A study for texture feature extraction of high-resolution satellite images based on a direction measure and gray level co-occurrence matrix fusion algorithm," Sensors, vol. 17, no. 7, p. 1474, 2017.

(Gagalowicz, 1983) : A. P. Gagalowicz, 1983,« Vers un modèle de texture», thèse de doctorat, université Pierre et Marie Curie, Paris VI, France.

(Oanh, 2009) : Nguyen Thi Oanh, 2009, « Localisation de symboles dans les documents graphiques », thèse de doctorat, Université de Nancy 2, France, 2009.

(Mohand, 2008) : Farid Mohand Oussaid, 2008, «Combinaison des données optiques et radar pour la cartographie de l'occupation du sol», mémoire de magister, Centre des Techniques Spatiales, Oran, 2008.

(Zahzah, 1992) : El-hadi Zahzah, 1992, «Contribution à la présentation des connaissances et leur utilisation pour l'interprétation automatique des images satellites», thèse de doctorat, Université Paul Sabatier, Toulouse, France, 1992.

(SAYAH , 1973) : N. E. H. SAYAH et S. DJELTI, « ETUDE DES METHODES D'ANALYSE DE

LA TEXTURE DES IMAGES MEDICALES ARM, » mém. de mast., Abou Bekr Belkaid university of Tlemcen, sept. 2017.

(HARALICK , 1973) : R. M. HARALICK, K. SHANMUGAM et I. H. DINSTEIN, « Textural features for image classification, » IEEE Transactions on systems, man, and cybernetics,no 6, p. 610-621, 1973.

(Kadar, 2010) : Bachir Kadar,2010, « Contribution d'un modèle Markovien pour la détection de changement dans les images satellitaires», mémoire de magister, Université des Sciences et de la Technologie d'Oran, 2010.

(Tonye et al., 2000) : Emanuel Tonye, Alain Akono Et Andre Ndi Nyoungui, 2000, « Le traitement des images de télédétection par l'exemple », Edition Gordon and Breach, Paris, France, 2000.

(Abadi, 2009) : Mohamed Abadi, Enguerran Grandchamp, 2009« Classification des couverts végétaux par analyse de textures, couleurs d'images satellites haute résolution», thèse de doctorat, Université Antilles GUYANE, 2009.

(Materka et al., 2001) : Andrzej Materka, Michal Strzelecki, 2001, «Texture analysis methods», a review, technical University of Lodz, Poland, 2001.

(Maenpaa , 2000) : T. Maenpaa, T. Ojala, M. Pietikainen, and M. Soriano, 2000, "Robust texture classification by subsets of local binary patterns " . In: Proc. ICPR. Vol. 3. IEEE, pp. 935–938, 2000.

(Ojala , 2002) : T. Ojala, M. Pietikainen, T. Maenpaa, "Multiresolution gray scaleand rotation invariant texture classification with local binary patterns". IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (7),971–987, 2002.

ملخص

البريد الإلكتروني وسيلة اتصال مستخدمة على نطاق واسع، ولكنها تواجه أيضًا مشكلة أمنية كبيرة: البريد العشوائي. تطورت هذه الرسائل غير المرغوب فيها إلى صورة غير مرغوب فيها، حيث يتم تضمين نص البريد العشوائي في الصور المرفقة برسائل البريد الإلكتروني. مرشحات الكشف التقليدية عن البريد العشوائي القائمة على النص غير فعالة في اكتشاف البريد العشوائي للصور. لحل هذه المشكلة، يقترح مشروعنا نظام كشف الصور غير المرغوب فيها بناءً على ثلاث طرق، باستخدام طريقة LBP بشكل أكثر تحديدًا، وطريقة GLCM والطريقة الهجينة بينهما (LBP + GLCM). يتم استخدام طريقتين للتعلم الآلي ، مثل SVM و KNN ، لإجراء التصنيف. ثم نقوم بمقارنة النتائج المختلفة التي تم الحصول عليها من خلال الأساليب والتقنيات المختلفة المستخدمة. تم إجراء اختبارات تجريبية على قاعدة بيانات حقيقية وتم الحصول على نتائج مرضية. النظام المطور قادر على تمييز صور البريد العشوائي عن الصور المشروعة (Ham)، وبالتالي تحسين اكتشاف البريد العشوائي للصور في رسائل البريد الإلكتروني.

Abstract

Electronic mail (e-mail) is a widely used means of communication, but it is also faced with a major security problem: spam. These unsolicited messages have evolved into image spam, where spam text is embedded in images attached to e-mails. Traditional text-based spam detection filters are ineffective at detecting image spam. To solve this problem, our project proposes an image spam detection system based on three methods, specifically using the LBP method, the GLCM method and the hybrid method that combines the two methods (LBP+GLCM). Two machine learning techniques, such as SVM and KNN, are used to perform classification. We then compare the different results obtained by the different methods and techniques used. Experimental tests on a real database have been carried out, and satisfactory results have been obtained. The system developed is capable of distinguishing spam images from legitimate (Ham) images, thus improving the detection of image spam in e-mails.

Résumé

Le courrier électronique (e-mail) est un moyen de communication largement utilisé, mais il est également confronté à un problème de sécurité majeur : les spams. Ces messages non sollicités ont évolué vers le spam image, où le texte du spam est intégré dans des images jointes aux e-mails. Les filtres de détection de spam traditionnels basés sur le texte sont inefficaces pour détecter le spam image. Pour résoudre ce problème, notre projet propose un système de détection de spam image basé sur trois méthodes, en utilisant plus spécifiquement la méthode LBP, la méthode GLCM et la méthode hybride qui combine les deux méthodes (LBP+GLCM). Deux techniques d'apprentissage automatique, telles que le SVM et KNN, sont utilisées pour effectuer une classification. Ensuite, nous comparons les différents résultats obtenus par les différentes méthodes et techniques utilisées. Des tests expérimentaux sur une base de données réelle ont été effectués, et des résultats satisfaisants ont été obtenus. Le système développé est capable de distinguer les images spam des images légitimes (Ham), améliorant ainsi la détection des spams image dans les e-mails.