CRYPTER UN MESSAGE NUMERIQUE

PROBLEMATIQUE SOCIETALE : LA COMMUNICATION

Cette activité permet d'appréhender les techniques de base en cryptologie. Ce processus peut être aisément transféré sur du texte, des images ….

CRYPTER UN MESSAGE NUMERIQUE

PROBLEMATIQUE SOCIETALE : LA COMMUNICATION

A - ANALYSER

A1- ANALYSER LE BESOIN : POURQUOI CRYPTER ?

Objectif de cette partie : **analyser** le besoin à l'origine de la cryptologie.

Comparer la solution retenue avec une autre solution possible.

La cryptographie est la science du codage des messages à l'aide de *codes secrets* ou de *clés*. Le codage des messages vise à en assurer la confidentialité, l'authenticité et l'intégrité.

Le cryptage permet de rendre l'information secrète. Les gouvernements, armées et industries utilisent ces technologies afin de protéger certaines informations, et considèrent pour cette raison la cryptologie comme une arme. Les individus utilisent à leur tour ces technologies, dans le cadre de leur vie privée. Le développement des outils informatiques permet aujourd'hui une sécurité accrue dans les échanges d'informations mais …. permet aussi un décryptage toujours plus facile par des personnes indélicates. Les principales techniques des pirates résident soient dans l'utilisation de la force brute (générer systématiquement les différents codes possibles jusqu'à trouver le bon) ou bien utiliser une technique fréquentielle qui permet de repérer certains motifs répétitifs dans le texte codé et d'en déduire la clef de cryptage. L'imagination des pirates étant sans limite d'autres techniques toujours plus sophistiqués

UNE TRIPLE PROBLEMATIQUE?

AUTHENTIFIER

Assurer au destinataire d'un message crypté que son émetteur est bien celui qu'il prétend être

CONFIDENTIALITE

assurer à l'émetteur du message crypté que son destinataire sera seul à pouvoir le lire. Certaines données confidentiels, dossier médical, données bancaires, code d'accès etc … doivent être rendus inintelligibles à

CRYPTER

Permet de répondre à une triple problématique.

Authenticité

assurer au destinataire d'un message crypté que son émetteur est bien celui qu'il prétend être.

Confidentialité

assurer à l'émetteur du message crypté que son destinataire sera seul à pouvoir le lire.

Intégrité

le contenu du message n'a subi aucune altération entre son envoi et sa réception

d'autres personnes. Le numérique se prête bien au cryptage de données sensibles.

INTEGRITE

le contenu du message n'a subi aucune altération entre son envoi et sa réception

PREMIERE PARTIE

Q1/ Aujourd'hui la cryptologie est utilisée dans la vie privée des individus au quotidien. Citer au moins Trois applications qui utilisent les techniques de chiffrement pour préserver une confidentialité du message numérique lors d'une communication (utilisé le document ressource securibox) ?

p.s. le terme communication doit être interprété au sens large c'est-à-dire échange de fichiers sonores, images, texte)

Q2/ Nous allons maintenant verbaliser le besoin. Compléter le diagramme suivant ? Puis le tableau de caractérisation (utiliser les mots suivants : totale – partielle – sans objet).

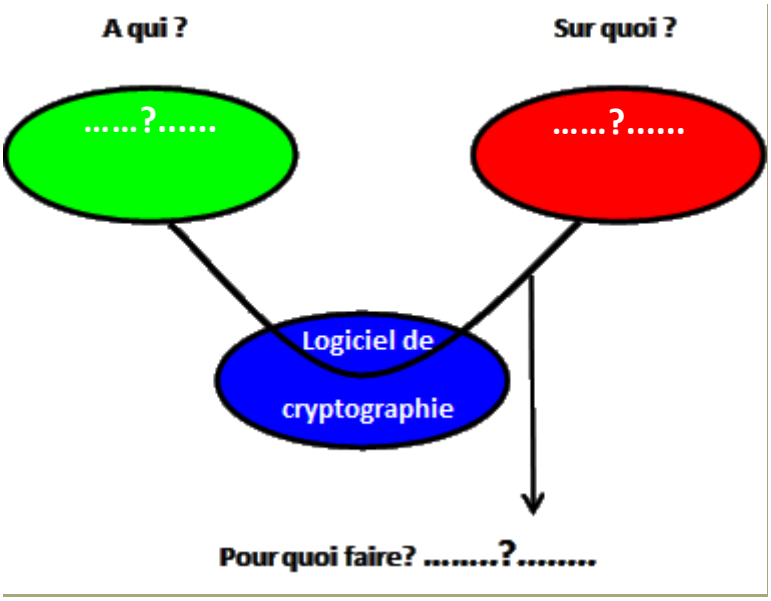


Tableau de caractérisation	
Critères	Valeur
Authenticité	
Confidentialité	
Intégrité	

Q3/ Finaliser le cahier des charges des prestations en complétant les trois affirmations suivantes :

Pourquoi le produit existe-t-il ? Parce que ……

Qu'est ce qui pourrait faire évoluer le besoin ? Que ……

Qu'est-ce qui pourrait faire disparaitre le besoin ? Que ……

Q4/ En vous aidant des documents supports Chiffre de Vigenère et Enigma , justifier la pertinence des techniques actuelles de chiffrement par rapport à des solutions tels que les deux précédentes qui pourraient

être revisités (autre tableau de substitution pour Vigenère ou rotor avec d'autres chemins électriques possibles).

A2 – ANALYSER LE SYSTEME

IDENTIFIER LES ELEMENTS TRANSFORMES ET LES FLUX

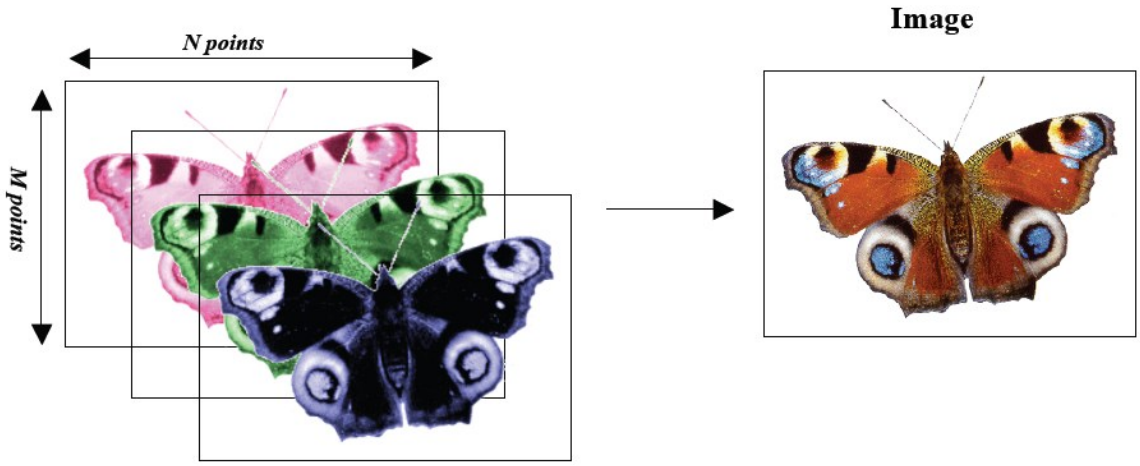
IDENTIFIER L'ORGANISATION STRUCTURELLE

Objectif de cette partie: **Décrire et analyser** le comportement d'un système.

Dans cette première partie de notre expérimentation nous allons mettre en œuvre un procédé de stéganographie (appelé aussi watermarking) toujours très utilisé aujourd'hui. Le principe est simple il s'agit de faire passer inaperçu un message dans un autre message.

Aux alentours de -600, Nabuchodonosor, roi de Babylone, employait une méthode originale : il écrivait sur le crâne rasé de ses esclaves, attendait que leurs cheveux aient repoussé, et il les envoyait à ses généraux. Il suffisait ensuite de raser à nouveau le messager pour lire le texte. Il s'agit bien de stéganographie à proprement parler et non pas de cryptographie : l'information est cachée et non pas codée.

Comment Matlab gère les images



Une image couleur est la superposition de 3 composantes de base (Rouge Vert et Bleu). Sous Matlab une telle image peut-être codée par un tableau tridimensionnel. Il correspond à la mise en cascade des 3 tableaux (2D : N*M) correspondant aux 3 composantes primaires (Rouge Vert et Bleu). Chacun de ces 3 tableaux primaires (aussi appelées « plans couleur ») contient le niveau de couleur pour chaque point de l'image considérée. En général chaque niveau de couleur est codé entre 0 (canal colorimétrique éteint) et 255 (canal colorimétrique maximum) ce qui correspond à 255^3 = 16 581 375 combinaisons de couleurs possibles.

PRINCIPE DU CODAGE ET DU DECODAGE

La technique mise en œuvre dans cette activité est très simple :

- soient deux images au format bmp

- la première se nomme image_conteneur.bmp

- la deuxième image_secrete.bmp

Le but est «d'incruster » l'image secrète dans l'image (anodine) du conteneur.

Le codage

Octet de l'image conteneur

b7	b6	b5	b4	b3	b2	b1	b0

Bit de poids fort — Bit de poids faible

Octet de l'image secrète

b7'	b6'	b5'	b4'	b3'	b2'	b1'	b0'

Bit de poids fort — Bit de poids faible

1ère étape

b7	b6	b5	b4	0	0	0	0

Bit de poids fort — Bit de poids faible

Les 4 bits de poids faibles sont mis à 0

0	0	0	0	b7'	b6'	b5'	b4'

Bit de poids fort — Bit de poids faible

L'octet de départ est décalé de 4 colonnes vers la droite et les 4 cases vides sont remplies de 0

2ème étape

b7	b6	b5	b4	b7'	b6'	b5'	b4'

Bit de poids fort — Bit de poids faible

On effectue le OU logique des deux octets. C'est l'octet **que je transmets**.

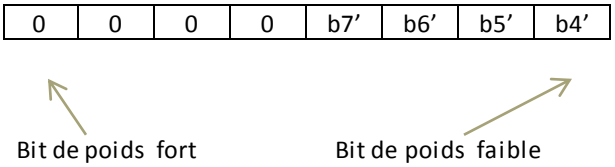
Le décodage

b7	b6	b5	b4	b7'	b6'	b5'	b4'

Bit de poids fort — Bit de poids faible

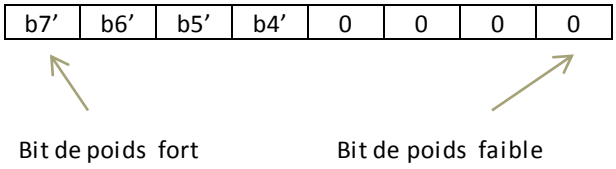
C'est l'octet que **je reçois**.

1ère étape



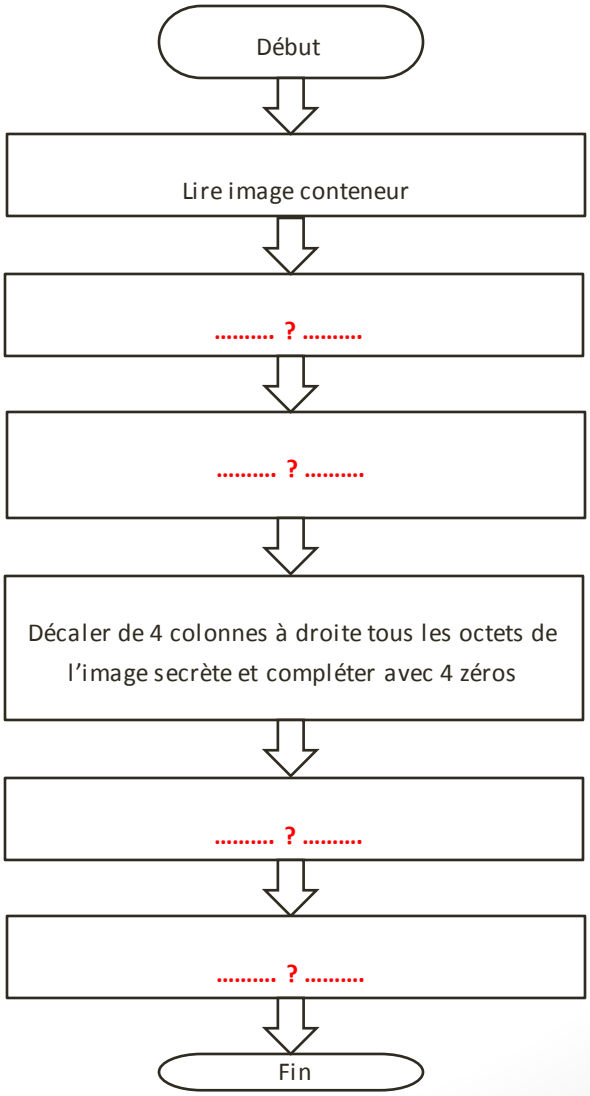
Je mets à 0 le quartet fort.

2eme étape

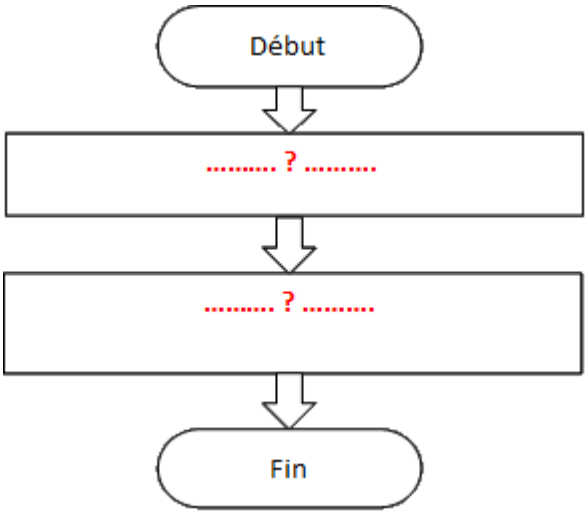


Je décale de 4 colonnes vers la gauche et je mets à 0 le quartet faible. L'image reconstruite a perdu en qualité par rapport à l'original.

Q5/ Compléter l'algorithme du codeur



Q6/ Compléter l'algorithme du décodeur



B-MODÉLISER

B2 PROPOSER OU JUSTIFIER UN MODELE

ASSOCIER UN MODELE A UN SYSTEME OU A SON COMPORTEMENT

B4 VALIDER UN MODELE

INTERPRETER LES RESULTATS OBTENUS

Objectif de cette partie: **Traduire** le comportement d'un système.

Vérifier la compabilité des résultats obtenus. Comparer les résultats obtenus.

Q7/ Ouvrir le programme  Matlab water_marking_eleves.m, compléter les lignes 17, 21 et 23 (algorithme du codeur) . Sauvegardez vos modifications. (Utilisez le document ressource langage Matlab pour compléter le programme).

Q8/ Compléter dans le programme Matlab water_marking_eleves.m, les lignes 28 et 29 (algorithme du décodeur). Sauvegardez vos modifications. Faites vérifier toutes vos modifications par le professeur. (Utilisez le document ressource langage Matlab pour compléter le programme).

Q9/ Exécuter le programme. Saisir au clavier image_conteneur.bmp puis image_secrete.bmp. Le résultat s'affiche dans la fenêtre « figure ». Imprimer vos résultats dans votre compte rendu. Faites vérifier vos résultats par le professeur. Corriger votre programme si les résultats ne sont pas acceptables.

Q10/ Dans le « workspace » de Matlab, double cliquer sur I et Ipfort, nous allons examiner quelques résultats et vérifier la conformité de notre programme. Les résultats s'affichent sous forme de tableau. Le premier octet de l'image I est égal à $97_{(10)}$ (en base 10) et Ipfort = $96_{(10)}$. Convertir ces deux octets en binaire. Quelle opération est effectuée ? Vérifier sur d'autres couples de valeurs (ligne 2 par exemple). Cela correspond-il à l'action 3 de votre algorithme de codage ? Conclure.

Q11/ Dans le « workspace » de Matlab, double cliquer sur J. Le premier octet de l'image J est égal à $219_{(10)}$. Convertir cet octet en binaire. Décaler l'octet vers la droite de 4 colonnes et compléter avec 4 zéros. Quelle valeur en décimale obtenez-vous ? Double cliquer sur Jdecaldroite, quelle est la valeur de l'échantillon ? Cela correspond-il à l'action 4 de votre algorithme de codage? Vérifier sur d'autres couples de valeurs (ligne 2 par exemple). Conclure.

Q12/ Examiner la valeur du 1er octet de l'image transmise (cliquer sur Image_transmise dans le workspace). Convertir en binaire cette valeur. Cette valeur est-elle conforme avec l'action 5 de votre algorithme de codage. Vérifier sur d'autres couples de valeurs (ligne 2 par exemple). Conclure.

Q13/ A partir de la représentation binaire trouvée à la question précédente, prendre le quartet de poids faible de l'image transmise et le décaler de 4 colonnes vers la gauche. Quel résultat en décimal obtenez-vous ? Cliquer sur Image_décodee dans le workspace. Cette valeur est-elle conforme avec l'action 2 de votre algorithme de décodage. Vérifier sur d'autres couples de valeurs (ligne 2 par exemple). Conclure.

A3 ANALYSE D'ECARTS ENTRE LE SOUHAITE, LE SIMULE ET LE REALISE

COMPARER LES RESULTATS EXPERIMENTAUX AVEC LES CRITERES DU CAHIER DES CHARGES ET INTERPRETER LES RESULTATS.

Objectif de cette partie : **analyser** les écarts avec les critères de caractérisation : authenticité, confidentialité, intégrité.

Le procédé mis en œuvre dans notre expérimentation est purement logiciel, nous considérons donc que le résultat simulé est égal au résultat réalisé, ce qui induit un écart nul entre le simulé et le réalisé.

Q14/ Les valeurs de pixels trouvées pour l'image décodée sont-ils identiques aux valeurs de l'image secrète ? Quelle peut être la conséquence sur l'image reconstruite ? Pensez-vous satisfaire le critère 3 intégrité (tableau des caractérisations Q3) ?

Q15/ Que pourriez-vous introduire comme modifications simple dans le programme pour satisfaire au critère d'intégrité ? (Enoncer le principe ou dessiner un algorithme de codage/décodage).

Q16/ Que pensez-vous de la satisfaction par votre programme informatique des critères tel que authenticité, confidentialité ? Indiquez notamment si ces critères sont satisfaits ? Suggérez une piste de réflexion qui permette de valider des deux critères essentielles ?

DEUXIEME PARTIE

B-MODÉLISER

B2 PROPOSER OU JUSTIFIER UN MODELE

ASSOCIER UN MODELE A UN SYSTEME OU A SON COMPORTEMENT

B4 VALIDER UN MODELE

INTERPRETER LES RESULTATS OBTENUS

Objectif de cette partie: **Traduire** le comportement d'un système.

Vérifier la compabilité des résultats obtenus. Comparer les résultats obtenus.

Q17/ A partir du document précédent complétez les motifs bi-pixels clef et bi-pixels image transmise (noircir les sous pixels mis à 0). Quelle opération logique effectuez-vous ?

Pixel image de départ	0 	1 	1 	0 
Nombre aléatoire	0	0	1	1
Codage				
Bi-pixels Clef				
Bi-pixels Image transmise				
Décodage				
Bi-pixels Image brute reconstruite				
Pixel Image reconstruite finale				

Q18/ Ouvrir le fichier  Matlab cryptographie_visuelle_eleves.m. Compléter les lignes 38 et 39 du programme afin de réaliser la fonction logique déterminée à la question précédente.

Q19/ En vous aidant du document ressource Notions de cryptographie visuelle. (notamment du chapitre Comment ça marche ?) Enoncez la relation logique entre les trois variables Image reconstruite, Clef, et Image transmise ? Rappelez la table de vérité de cette fonction logique ? En déduire le motif du bi-pixel Image brute reconstruite (ligne 3 du tableau)?

a	b	S
0	0	
0	1	
1	0	
1	1	

Q20/ A l'aide du document ressource Notions de cryptographie visuelle, énoncez la relation logique entre les composantes du bi-pixel Image reconstruite et le pixel de l'image final ? Rappelez la table de vérité de cette fonction logique ? En déduire le motif du pixel Image reconstruite (ligne 4 du tableau)? Conclure sur le processus de codage et de décodage ?

a	b	S
0	0	
0	1	
1	0	
1	1	

Q21/ Compléter la ligne 47 du programme. Quelle est la signification de la variable image_recons ?

image_recons c'est le : cocher une case

☐ Pixel image de départ ☐Bi-pixels Clef
☐Bi-pixels Image transmise
☐ Bi-pixels Image brute reconstruite ☐Pixel final

Q22/ Exécuter le programme. Saisir au clavier image de test.jpg. Le résultat s'affiche dans la fenêtre « figure ». Imprimer vos résultats dans votre compte rendu. Faites vérifier vos résultats par le professeur. Corriger votre programme si les résultats ne sont pas acceptables.

Q23/ Les dimensions de l'image transmise ne sont pas identiques au format de l'image originale (ou finale), cela est-il normal ? Quel inconvénient cela peut-il représenter lors d'une transmission via un réseau type internet ?

A3 ANALYSE D'ECARTS ENTRE LE SOUHAITE, LE SIMULE ET LE REALISE

COMPARER LES RESULTATS EXPERIMENTAUX AVEC LES CRITERES DU CAHIER DES CHARGES ET INTERPRETER LES RESULTATS.

Objectif de cette partie : **analyser** les écarts avec les critères de caractérisation : authenticité, confidentialité, intégrité.

Le procédé mis en œuvre dans notre expérimentation est purement logiciel, nous considérons donc que le résultat simulé est égal au résultat réalisé, ce qui induit un écart nul entre le simulé et le réalisé.

Q24/ Examiner dans le workspace de Matlab la valeur de quelques pixels sur l'image originale en noir et blanc et sur l'image finale (choisissez des pixels avec les mêmes coordonnées dans les images). Quelle est votre conclusion ?

Q25/ Conclure sur le procédé de cryptage, notamment vis-à-vis des trois critères authenticité, confidentialité, intégrité.