PREMIER COLLOQUE IMAGE

Traitement, Synthèse, Technologie et Applications

BIARRITZ – Mai 1984 –

CODAGE ET PROTECTION DES INFORMATIONS DANS UN SYSTEME DE TRANSMISSION D'IMAGE FONCTIONNANT EN TEMPS REEL

INFORMATION CODING AND SAFETY IN REAL-TIME TRANSMISSION SYSTEM

MASSIP-PAILHES L. - PAYRISSAT R.

Laboratoire C.E.R.F.I.A. Université Paul Sabatier 118 route de Narbonne 31062 TOULOUSE CEDEX

RESUME

Les critères de qualité d'un système téléphoto utilisé pour la transmission d'images digitalisées (iconiques ou graphiques) sont caractérisés par la minimisation du temps entre l'émission et la reconstitution complète de l'image avec une qualité psychovisuelle acceptable. Les images considérées sont du type iconiques à haute résolution (20 ppmm).

Du fait de leur grande simplicité de mise en oeuvre, les systèmes de compression d'images à codage prédictif, du type MICD, sont particulièrement bien adaptés à la transmission en temps réel. Cependant, les taux de compression théoriques obtenus sont inférieurs à 3. Des modifications ont permis de tripler les performances du codage par MICD et d'obtenir ainsi des taux de compression comparables à ceux fournis par des méthodes globales : il s'agit de la compression par MICD adaptée,étendue (MICDAE).

Malheureusement, ces systèmes se caractérisent par une vulnérabilité importante aux erreurs de transmission. La propagation d'erreurs bidimensionnelle -plus ou moins importante suivant la prédiction utilisée et le mode de codage binaire des informations à transmettre- ne permet pas, en général, une reconstitution correcte de l'image émise.

Apres une description sommaire de la compression par MICDAE, les problèmes posés par le codage des informations de source, la vulnérabilité et la protection contre les erreurs de transmission ont été étudiés.

SUMMARY

The quality criteria of a telephoto system used for transmission of digitalized images (multilevels or graphic) are caracterized by the minimisation of the time between the image emission and its complete reconstruction with a good visual quality. The images studied are high resolution type (20 ppmm).

Because of their high working up easiness, the data compression system using predictif codage, such as DPCM are specially well adapted to real time transmission. Nevertheless, the theorical compression ratio are inferior to 3. Some modifications allowed as to triple the performances of the DPCM codage and to get compression ratio that can be compared to those given by global methods : we used compression by DPCM adapted extended (DPCMAE).

Infortunately, those systems are caracterized by a great sensibility to errors transmission. The propagation of bidimensional errors - more or less important according to the used predictor and the binary codage mode of the informations to be transmetted - generally does not allow a poper reconstruction of the initial image.

After a brief description of the compression by DPCMAE, the problems caused by the source information codage, the sensibility and the protection against the trasmission errors are dealt with.

CODAGE ET PROTECTION DES INFORMATIONS DANS UN SYSTEME DE TRANSMISSION D'IMAGE FONCTIONNANT EN TEMPS REEL

MASSIP-PAILHES L. - PAYRISSAT R.

INFORMATION CODING AND SAFETY IN REAL-TIME TRANSMISSION SYSTEM

La compression par MICDAE (2) associe un codage des longueurs de plage au codage des écarts MICDA. Le principe est illustré par le schéma ci-dessous.

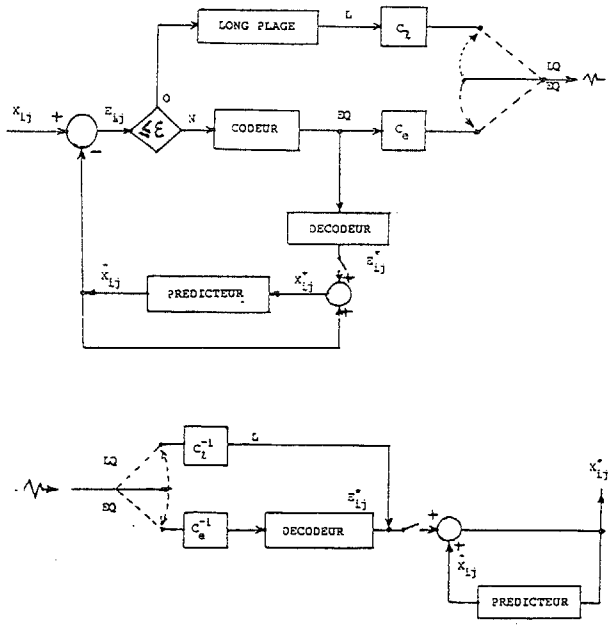


Figure 1 : Principe de la compression par MICDAE

Si l'écart E est, en valeur absolue, inférieur ou égal à un seuil de tolérance ε fixé (ε=1,2,...) la valeur prédite est substituée à la valeur de l'intensité exacte ; dans ce cas, aucune information n'est transmise. Dès qu'un écart MICD satisfera $|e| > \varepsilon$, une plage de saut sera mise en évidence. Sa longueur l_s suivie de l'écart quantifié Eq seront ensuite codés au moyen des fonctions de codage C_l et C_e respectivement, qui sont liées aux types d'images à transmettre (iconiques ou graphiques). Dans l'application qui nous intéresse, ces images sont iconiques, noir et blanc à 32 niveaux de gris par pixel ; leur format est de 250 mm x 250 mm et comportent 5 000 lignes de 5 000 points chacune.

Il sera envisagé dans ce qui suit le problème du codage binaire des informations à transmettre qui constituent la source et la protection contre les erreurs de transmission.

I - CODAGE DE SOURCE.

Il s'agit ici de définir un codage sous optimal qui affecte le moins possible les performances (taux de compression) obtenues par la compression MICDAE.

L'efficacité du codage dépend du taux de compression réel (T.C.R.) défini par le rapport du nombre d'éléments binaires nécessaires pour coder les informations originales, au nombre d'éléments binaires qui codent les informations transmises. Le code utilisé devra donc maximiser le taux de compression réel qui ne peut être accessible que par simulation complète du système (figure 1). De plus, la réalisation du codeur et du décodeur associé devra être suffisamment simple afin de ne pas altérer le temps de transmission.

1. Choix d'un codage déchiffrable sous-optimal.

Les informations consituant la source comprennent d'une part 6 niveaux d'écarts quantifiés et d'autre part, les longueurs l_s de plages de saut ($1<l_s<5000$).

Pour coder ces informations, le codage unidimensionnel d'Huffman a été utilisé. Avec ε=1, le taux de compression réel est égal à 5,054 et est donc très proche du taux de compression théorique qui vaut 5,094. Cependant, contrairement au codage par plage d'images graphiques où plages d'écarts et plages de saut alternent (7), les codes obtenus ne permettent pas un déchiffrage correct et il y a ambiguïté en ce qui concerne le décodage de la suite écart-écart ou écart-longueur de saut. Autrement dit, ce codage ne permet pas de reconstruire au récepteur l'alternance écart-plage de saut émise par l'émetteur. Afin de préserver la propriété de déchiffrabilité au décodage, deux méthodes ont été étudiées et comparées.

a) Code d'Huffman unique.

Les écarts et les longueurs de saut seront codés avec des mots appartenant à un même code.

Définissons plus précisément les informations source à coder.

Soient (E,P_1) et (L,P_2) les ensembles probabilité d'écarts et de longueurs de saut respectivement. Si P_e désigne la probabilité pour qu'un point soit transmis en écart MICD et P_s la probabilité de transmettre un saut, alors la source S est donnée par

S = E U L avec les probabilités associées

$$P_r\,[S=\sigma] = P_e P_1 \Psi_E(\sigma) + P_s P_2 \Psi_2(\sigma)$$

où Ψ_E et Ψ_L désignent les fonctions caractéristiques de E et L respectivement.

L'ensemble S ainsi probabilisé est codé de façon optimale par l'algorithme d'Huffman. Pour ε=1 ou 2, les résultats obtenus en ce qui concerne les taux de compression réels figurent dans le tableau 1 ci-dessous (colonne a).

b) Séparation.

Afin de faire apparaître la règle d'alternance comme dans le cas d'images binaires, nous pouvons soit :

- indiquer la fin d'une séquence d'écarts par un code particulier annonçant le codage d'une plage (Tableau 1, colonne c)

- introduire un codage de plage de longueur nulle entre deux écarts consécutif (Tableau 1 colonne b).

ε	T C T	T C R		
		Code HU a	Code HS b	Code HS c
1	5.094	3.703	4.253	3.707
2	8.200	6 192	7.316	6.218

Tableau 1. Efficacités comparées de codages compatibles avec le mode de compression par MICDAE.

L'étude du codage de source a montré d'une part, la sensibilité généralement importante du taux de compression réel aux modifications du code obtenu afin de garantir la propriété d'alternance écart-plage de saut. Le meilleur résultat a donc été obtenu en introduisant un séparateur (mode code de saut nul) dans le code des longueurs de saut.

CODAGE ET PROTECTION DES INFORMATIONS DANS UN SYSTEME DE TRANSMISSION D'IMAGE FONCTIONNANT EN TEMPS REEL. MASSIP-PAILHES L. - PAYRISSAT R.
INFORMATION CODING AND SAFETY IN REAL-TIME TRANSMISSION SYSTEM

2. Code tronqué.

Le nombre important de mots codes de longueur de saut ne permet pas une exploitation aisée pour coder et décoder des sauts importants.

Une modification du code obtenu du type Huffman tronqué [7] a été effectuée de manière à favoriser une manipulation par octets des mots codes. Pour ε égal à 1, ces codes sont représentés dans le tableau 2.

* Les mots initiaux codent les plages de saut de longueurs inférieures ou égales à 18.

* Pour les longueurs de saut supérieures à 18, le mot de composition 000101 est utilisé. Sa probabilité d'occurrence est donnée par

$$\sum_{l_s>18} Pr\left[L=l_s\right].$$

Niveaux	Probabilités	Mots codes
1	,08625	0010
2	,19780	01
3	,49550	1
4	,16610	000
5	,03895	00110
6	,01540	00111

(a)

Niveaux	Probabilités	Mots codes
0	,28885	01
1	,19095	11
2	,12430	100
3	,08695	0000
4	,06320	0011
5	,04920	1011
6	,03630	00100
7	,02935	00101
8	,02345	10101
9	,01865	000110
10	,01515	101000
11	,01225	0001000
12	,01020	0001110
13	,00750	0001111
14	,00655	1010011
15	,00545	00010010
16	,00485	00010011
17	,00400	10100100
18	,00330	10100101
19	,01940	000101

(b)

Codesde Huffman tronqué

(a) Ecarts

(b) Plages de recopie

Figure 1

Ce codage a été effectué en considérant un champ de bits variables dont la longueur est codée sur 2 bits.

La structure des mots codes est alors représentée à la figure 2.

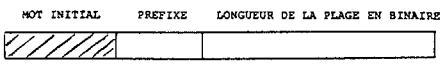


Figure 2. Codage des longueurs de sauts importants.

Dans le cas où ε est égal à 1, le codage de l_s s'est effectué comme suit :

$1_s \leq 18$ mot initial (voir tableau 1)

$18 < l_s \leq 63$ mot de composition + préfixe 11 + (l_s-18) codé sur 6e.b.

$64 \leq l_s \leq 255$ mot de composition + préfixe 01 + (l_s-64) codé sur 8e.b.

$256 \leq l_s \leq 1023$ mot de composition + préfixe 10 + (l_s-256) codé sur 10e.b.

$l_s > 1024$ mot de composition + préfixe 00 + (l_s-1024) codé sur 12e.b.

Le principe de la transmission est alors le suivant : afin d'initialiser le prédicteur, l'intensité du premier point de chaque ligne est transmise, codée sur 5 e.b. (c'est le mot de recalage en amplitude MRA). La longueur codée du saut jusqu'au premier point d'écart MICDA rencontré est ensuite émise. Après codage de cet écart, le processus se poursuit jusqu'à la fin de la ligne.

Sachant que la première information après MRA correspond à un mot code de longueur de saut, le décodeur reconstitue la ligne émise sans ambiguïté.

II - PROTECTION CONTRE LES ERREURS DE TRANSMISSION.

Le canal de transmission sur lequel transitent les informations codées est du type binaire symétrique ; les probabilités d'apparition d'erreurs aléatoires indépendantes et d'erreurs de coupure (longueur inférieure ou agale à 8) sont égales respectivement à 10^{-4} et 10^{-6}.

Du fait de l'utilisation de mots code de longueur variable pour transmettre les informations d'écarts et de longueurs de saut, l'effet des erreurs a généralement deux conséquences sur la qualité de l'image restituée :

* La première -la plus probable- consiste en une erreur de synchronisation entrainant une impossibilité de reconstituer l'image émise.

* La seconde aboutit à une reconstitution locale erronée de l'image. Ce cas peut arriver lorsqu'une erreur aléatoire ou de coupure survient sur MRA ou lorsqu'un mot code d'écart est transformé en un autre mot code de même nature. De par le mode de compression utilisé, il en résulte alors une propagation d'erreurs bidimensionnelle.

Pour ces types d'erreurs, deux modes de protection peuvent être envisagés : le masquage et la correction. Ces méthodes consistent à introduire une redondance ayant pour effet une diminution du taux de transmission à l'émetteur. De plus, le temps de transmission peut s'accroître de façon importante si la complexité des algorithmes de décision mis en oeuvre au récepteur nécessite des temps de réponse non négligeables.

L'objectif à atteindre étant l'obtention d'un temps de transmission minimal, les méthodes de protection contre les erreurs et les algorithmes associés devront allier la rapidité d'exécution, à la simplicité de mise en oeuvre qui conditionne le coût de réalisation.

1. Masquage des erreurs.

Dans la transmission d'images iconiques par MICDE, le masquage des erreurs sera effectué par ligne: le récepteur reconnaît chaque ligne grâce à l'adjonction d'un mot de synchronisation de fin de ligne (MSL). La détection d'erreurs est basée sur la comparaison du nombre de points composant une ligne au nombre de points reconstitués, après avoir reconnu MSL. Le masquage s'effectue par recopie de la ligne précédemment transmise.

Une erreur de transmission intervenant sur un mot de synchronisation entraîne la perte d'une ligne.

a) Recherche du mot de synchronisation de ligne.

Cette recherche entraine la détermination de la configuration minimale d'un mot de synchronisation identifiable sans ambiguïté dans le monoïde libre engendre par les mots du code en tenant compte de la règle d'utilisation (alternance plage-écarts).

Nous avons modifié les codes de Huffman de façon à rendre identifiable une séquence constante, cette solution étant facilement généralisable.

b) Résultats des simulations (Photo aérienne 512 x 512).

Les erreurs de transmission (aléatoires ou de

coupure) ont été simulées par un générateur de nombres pseudo-aléatoires. Elles ne sont intervenues qu'à partir de la 256e colonne de l'image transmise, c'est à dire sur la moitié gauche de l'image.

* Pour $\varepsilon = 1$, 115 lignes sur 256 ont été erronées, 112 ont été mansquées, 3 lignes erronées n'ont donc pas été détectées. La photographie montrant l'image restituée est présentée figure 3 (a).

Le taux de compression réel est égal à 3,725.

* Pour $\varepsilon = 2$, 86 lignes sur 256 sont erronées et masquées.

Le taux de compression réel est de 5,910.

Figure 3 a. - Image restituée pour $\varepsilon = 1$ sans correction

Figure 3 b. - Image restutuée pour $\varepsilon = 1$ avec correction

2. Méthode mixte.

La mauvaise qualité des images reçues nous a amené à associer au masquage, une méthode de correction.

Les contraintes concernant le temps de transmission suggère l'utilisation d'un (n,k) code de bloc à haut rendement, c'est à dire tel que le taux de transmission

$$R = \frac{k}{n} \text{ soit proche de 1.}$$

Ce code devra être choisi parmi ceux qui corrigent :

- soit les erreurs de coupure de longueur inférieure ou égale à 8.(Codes de Fire, de Burton, codes convolutionnels BPM ou d'Iwadare),

- soit les erreurs aléatoires de poids t avec t = 1, 2, 3 ... (Codes de Hamming, BCH, convolutionnels ...).

- soit les deux types d'erreurs mentionnés ci-dessus. (Code par entrelacement, codes de Reed-Solomon, codes BCH).

La distribution des erreurs obtenue lors de la simulation de la transmission par masquage a montré que, par bloc de 500 bits,

81% des blocs erronés le sont par des erreurs de poids 1

13% par des erreurs de poids 2 qui ne sont pas des coupures

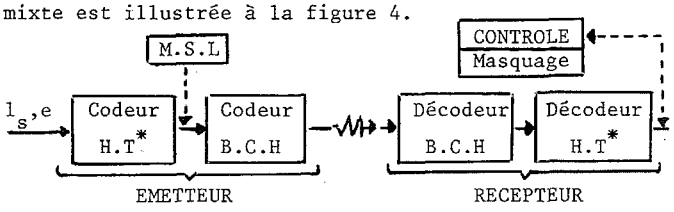
4% par des erreurs de poids ≥ 3 qui ne sont pas des coupures

et 2% par des erreurs de coupure.

Ainsi, la probabilité d'erreurs résiduelles obtenue en utilisant un code de longueur inférieure ou égale à 500 et correcteur de 2 erreurs sera négligeagle.

a) Choix du code correcteur.

Le code retenu a été le (255, 239) code de Bose-Chaudhuri-Hocquenghem correcteur de 2 erreurs. Son taux de transmission est égal à 0,94. Les erreurs résiduelles -affectant moins de 6% des lignes- seront détectées et masquées. Le principe de la transmission mixte est illustrée à la figure 4.



* H.T = Huffman tronqué

Figure 4. Synoptique de la transmission mixte.

Pour les codes BCH, le codeur est constitué par un simple circuit division. La description détaillée du codeur et du décodeur pour le (255, 239) est donnée dans [6], ainsi que la méthode permettant de déterminer le cablâge correspondant aux polynômes localisateurs d'erreurs qui permettent le décodage temps réel des informations transmises.

Pour le (255, 239) code de BCH choisi, les circuits de codage et de décodage ont été calculés et simulés.

Le codeur comprend :

1 registre à 16 bits
10 additionneurs (ou exclusif)
1 porte ET

Le décodeur utilise :

1 registre à 255 bits
3 regristres à 8 bits
110 additionneurs
34 porte ET
} circuit de calcul

2 registres 8 bits
24 portes ET
18 additionneurs
} circuit de correction

1 porte NON-ET

Un compteur modulo 255 sera de plus nécessaire pour gérer le transfert des a_i et pour la remise à zéro du circuit de calculs.

b) Résultats.

Pour $\varepsilon = 1$, 4 lignes ont été recopiées (masquage) alors que pour $\varepsilon = 2$, seulement 2 recopies se sont produites.

Chaque recopie de ligne correspond à une erreur de coupure, excepté une, qui est relative à un modèle d'erreur non corrigible de poids 3 survenue à la 436e ligne (ε=1).

Les taux de compression réels sont respectivement 3,491 et 5,539 pour $\varepsilon = 1$ et 2.

L'image restituée pour $\varepsilon = 1$ est présentée figure 3 b.

En résumé, le tableau 3 donne les taux de compression réels obtenus par les différentes méthodes :

E	Coefficient de compression				
	Théorique	Huffman	Huffman réduit	Sans correction	Avec correction
1	5,094	4,253	4,178	3,725	3,491
2	8,200	7,316	7,178	5,910	5,539

Tableau 3. Récapitulatif des performances obtenues

CONCLUSION.

Compte tenu des caractéristiques statistiques de la distribution d'erreurs du canal de transmission, l'utilisation d'un code correcteur d'erreurs a permis d'obtenir une probabilité d'erreurs résiduelles suffisamment faible pour qu'une méthode de masquage soit utilisable sans dégradation apparente (voir figure 3).

Du fait que les algorithmes de codage et de décodage câblés travaillent à la vitesse de la ligne, les taux de compression réels obtenus (tableau 3) correspondent à une réduction effective du temps de transmission dans le même rapport. En utilisant des résolutions d'images bien plus faibles, il est donc permis d'envisager la transmission, en temps réel, d'images animées.

De plus, le contexte de transmission mixte facilite le choix d'une méthode cryptographique destinée à se protéger contre un environnement hostile. En effet, la compression d'image a pour effet d'accroître la "distance unité" définie par SHANNON [5] et par conséquent d'augmenter la sécurité potentielle d'un chiffre. D'autre part, comme l'ont montré E.R. BERLEKAMP [1] et Mc ELIECE [4] le problème général du décodage des codes linéaires correcteurs d'erreurs est NP-Complet c'est à dire que l'opération de déchiffrement peut être rendu rédhibitoire [3].

BIBLIOGRAPHIE.

1. E.R. BERLEKAMP - R.Mc ELIECE - HENK Van TILBORG.
"On the inherent intractability of certain coding problem"
IEEE Trans. on Inf. Theory. Vol. IT-24 1978 (March).

2. S. CASTAN - L. MASSIP-PAILHES - J.J. BALAND
"Image coding system an adaptive DPCM"
5ème Congrès Patern Recognition. MIAMI 1980

3. M.R. GAREY and D.S. JONHSON.
"Computers and Intractability : A guide to the theory of NP-Completeness"
San Francisco : Freeman 1978.

4. Mc ELIECE R.J.
"A public-key cryptosystem based on algebric coding theory".
DSN Progress. Jet Propulsion Lab. 1978

5. MARTIN E. HELLMAN.
"An extension of the Shannon Theory Approach to Cryptography".
IEEE Trans. on Inf. Theory. Vol. IT 23. 1977

6. R. PAYRISSAT.
"Compression d'images et transmission avec protection contre les erreurs".
Thèse de 3ème cycle 1980.

7. U. ROTHGORDT - G. AARON - G. RENELT.
"One dimensional coding of black and white facsimile pictures".
Acta Electronica 1978.