Tatouage haute capacité dans des images chiffrées

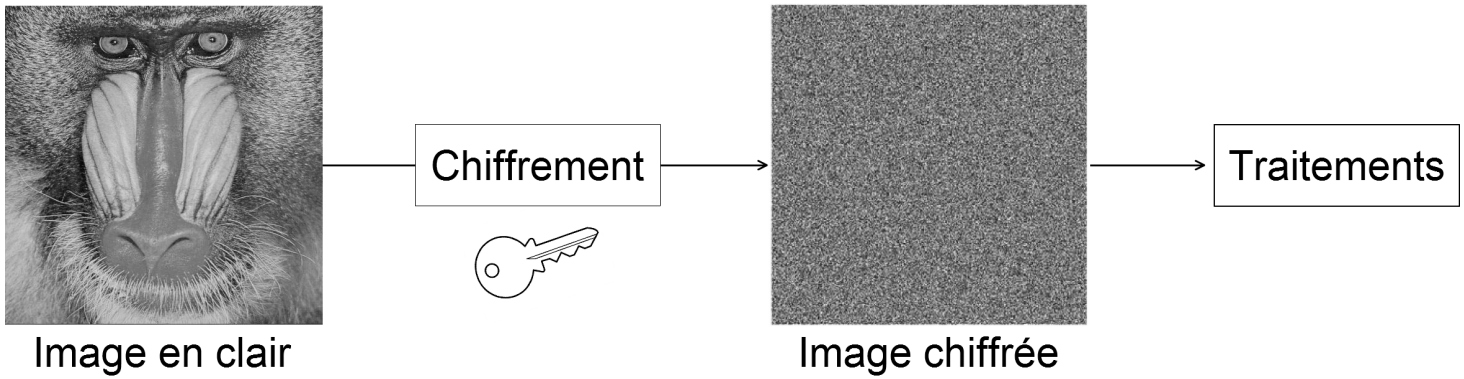
Pauline PUTEAUX

LIRMM - Équipe ICAR
Stage encadré par William PUECH

19 juillet 2016

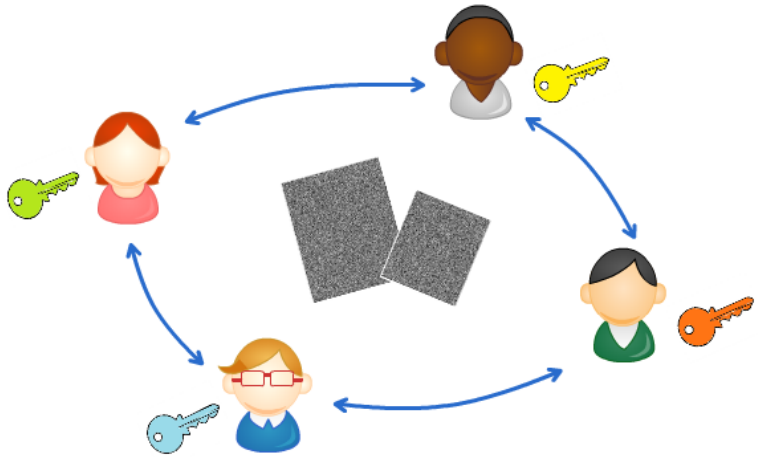
Traitement des images dans le domaine chiffré

- Problème de la sécurité des données numériques
- Beaucoup sont transférées ou archivées sous forme chiffrée
- Nécessité de les analyser et de les traiter sans la clef



Applications visées

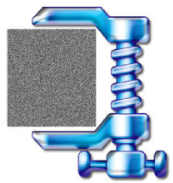
Partage d'images secrètes entre plusieurs personnes (VSS)



Indexation et recherche d'images ou des vidéos dans des BDD chiffrées

Insertion de données cachées dans des images chiffrées

Recompression d'images ou de vidéos crypto-compressées



Insertion de données réversible dans des images chiffrées

Définition

- Méthode efficace pour dissimuler des données dans le domaine chiffré sans connaître le contenu original de l'image.
- Après l'extraction du message, il doit être possible de reconstruire l'image originale sans altération.
- Nécessaire de trouver le meilleur compromis entre capacité de dissimulation et qualité de l'image reconstruite.

Insertion de données réversible dans des images chiffrées

Deux types d'approches [1] :

1. **VRAE** Libérer l'espace nécessaire pour dissimuler l'information après le chiffrement de l'image
2. **RRBE** Réserver de la place avant le chiffrement

Ces méthodes peuvent être [2] :

1. **Jointes** L'extraction des données et la reconstruction de l'image se font simultanément
2. **Séparatives** La reconstruction de l'image se fait après l'extraction des données

[1] K. Ma, W. Zhang, X. Zhao, N. Yu et F. Li

Reversible data hiding in encrypted images by reserving room before encryption

IEEE Transactions Inf. Forensics Security, vol. 8.3, p.553-562, 2013

[2] W. Zhang, K. Ma et N. Yu

Reversibility improved data hiding in encrypted images

Signal Processing, vol. 94, p.118-127, 2014

Etat de l'art

Méthode proposée en 2008 [1]

- Analyse de l'écart type pour reconstruire l'image originale sans erreurs
- Dissimulation d'un bit par bloc 4×4 (payload $= 0.0625$ bpp)

Analyse de la prédiction

- Technique la plus utilisée dans les méthodes récentes
- Exploiter la corrélation entre un pixel et ses voisins
- Généralement, remplacement du ou des bit(s) les moins significatifs (LSB)

[1] W. Puech, M. Chaumont et O. Strauss

A Reversible Data Hiding Method for Encrypted Images

Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, p : 68191E-1-68191E-9, 2008

Etat de l'art

Remarques

- Aucune des méthodes proposées ne permet de combiner haute qualité visuelle et grande capacité de dissimulation
- Méthodes considérées comme réversibles alors que PSNR $\neq \infty$
- Dans [1], haute capacité de dissimulation mais altération de l'image originale (PSNR $\approx$ 40 dB)
- Dans [2], Wu et Sun proposent une "haute" capacité de dissimulation alors qu'on ne peut cacher que 0.1563 bit par pixel

[1] K. Ma, W. Zhang, X. Zhao, N. Yu et F. Li
Reversible data hiding in encrypted images by reserving room before encryption
IEEE Transactions Inf. Forensics Security, vol. 8.3, p.553-562, 2013

[2] X. Wu et W. Sun
High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error
Signal Processing, vol. 104, p.387-400, 2014

Notre approche

Prédiction des bits les plus significatifs (MSB)

- Prédire les MSB plus simple que les LSB et tatouer les MSB ne pose pas de problème dans le domaine chiffré
- Analyse de l'image originale pour détecter les erreurs de prédiction
- Deux approches :
  1. Pré-traitement de l'image originale pour éviter toutes les erreurs de prédiction, chiffrement de l'image et tatouage de tous les pixels
  2. Construction d'une carte de localisation des erreurs de prédiction, chiffrement de l'image et adaptation du message à insérer

Approche très haute capacité - Schéma général (1)

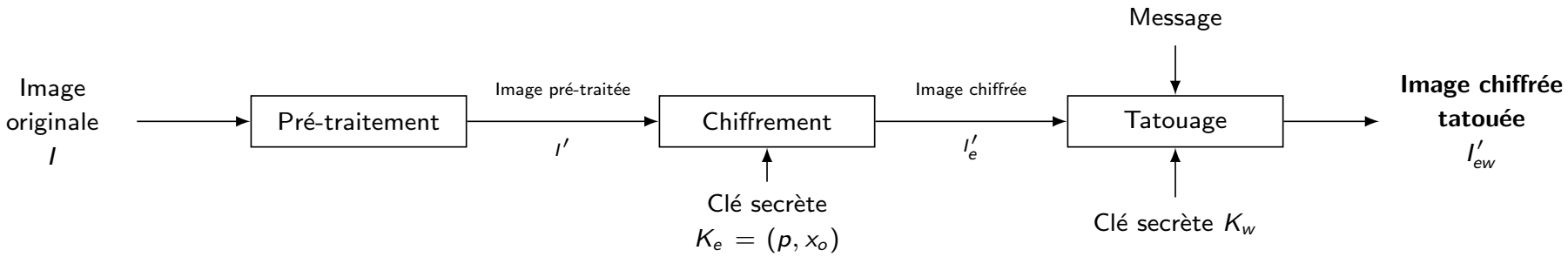


FIGURE – Chiffrement et tatouage

Approche très haute capacité - Pré-traitement

begin
  foreach *pixel* $p(i,j)$ **do**
    $inv(i,j) \leftarrow (p(i,j)+128)\%256$
    if *première ligne ou première colonne* **then**
      traitement spécial
    end
    else
      $pred(i,j) \leftarrow \frac{p(i-1,j)+p(i,j-1)}{2}$
    end
    if $|\ pred(i,j)-p(i,j)\ | \geq |\ pred(i,j)-inv(i,j)\ |$ **then**
      if $p(i,j) < 128$ **then**
        $p'(i,j) = pred(i,j) - 63$
      end
      else
        $p'(i,j) = pred(i,j) + 63$
      end
    end
    else
      $p'(i,j) = p(i,j)$
    end
  end
end

Algorithme 1 : Algorithme de pré-traitement

Approche très haute capacité - Chiffrement et tatouage

Chiffrement

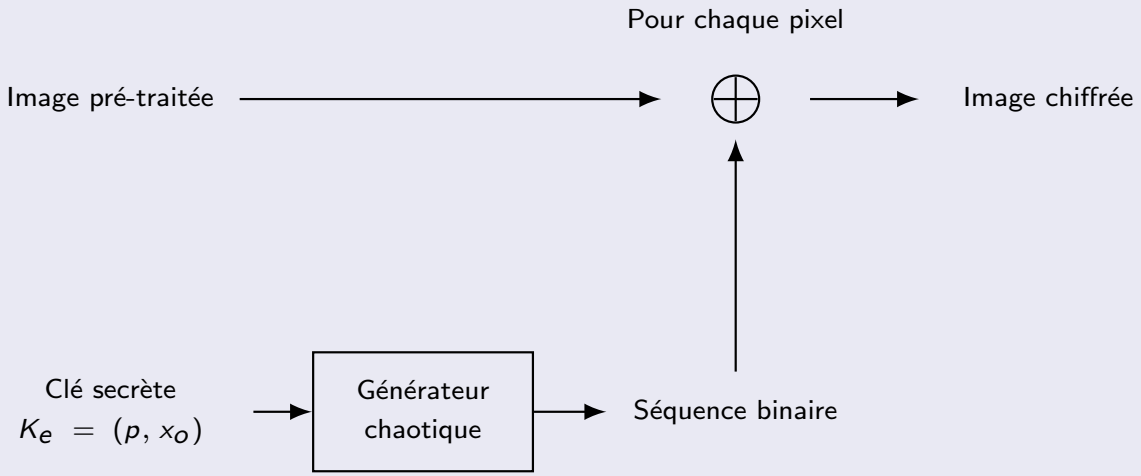


FIGURE – Schéma général du chiffrement

Tatouage

$$p'_{ew}(i,j) = b_l \times 128 + (p'_e(i,j) \bmod 128)$$

Approche très haute capacité - Schéma général (2)

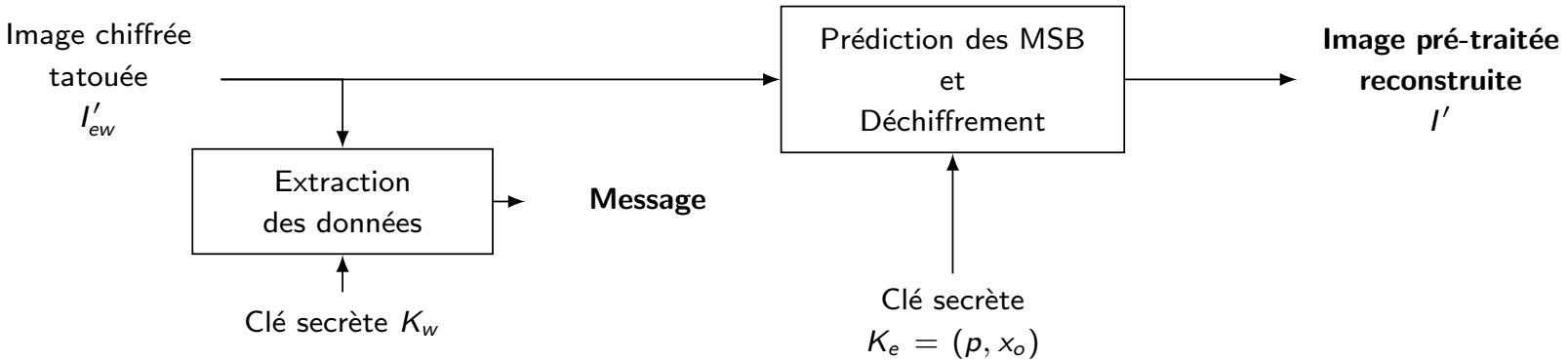
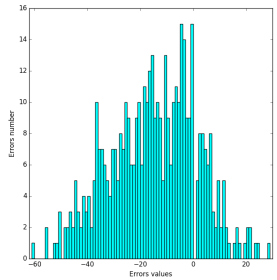


FIGURE – Extraction et reconstruction

Approche très haute capacité - Résultats

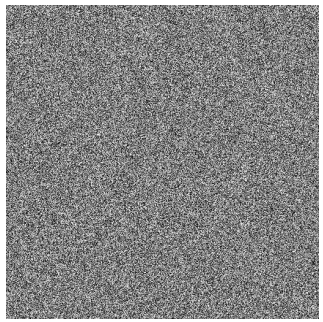
(a)

(b)



(c)

(d)



(e)

(f)

FIGURE – Illustration de notre méthode, payload = 1 bpp. a) Image originale I, b) Emplacement des erreurs, nombre d'erreurs = 448 (0.2%), c) Histogramme des erreurs de prédiction estimées, d) Image pré-traitée I', PSNR = 48.67 dB, e) Image chiffrée tatouée I_{ew}, f) Image reconstruite I', PSNR = 48.67 dB, SSIM = 0.9998

Approche très haute capacité - Résultats

	Meilleur cas (9.2%)	Pire cas	Moyenne
Nombre d'erreurs de prédiction des MSB dans l'image originale	0%	3.2%	0.3%
PSNR (dB)	$+\infty$	36.06	54.84
SSIM	1	0.9966	0.9998

TABLE – Mesures de la qualité des images sur une base de 500 images

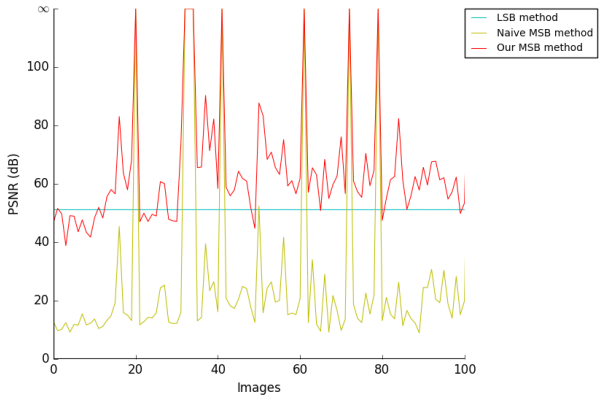


FIGURE – Comparaison de la qualité des images reconstruites entre notre méthode et d'autres avec la même capacité (1 bpp)

Approche totalement réversible - Schéma général (1)

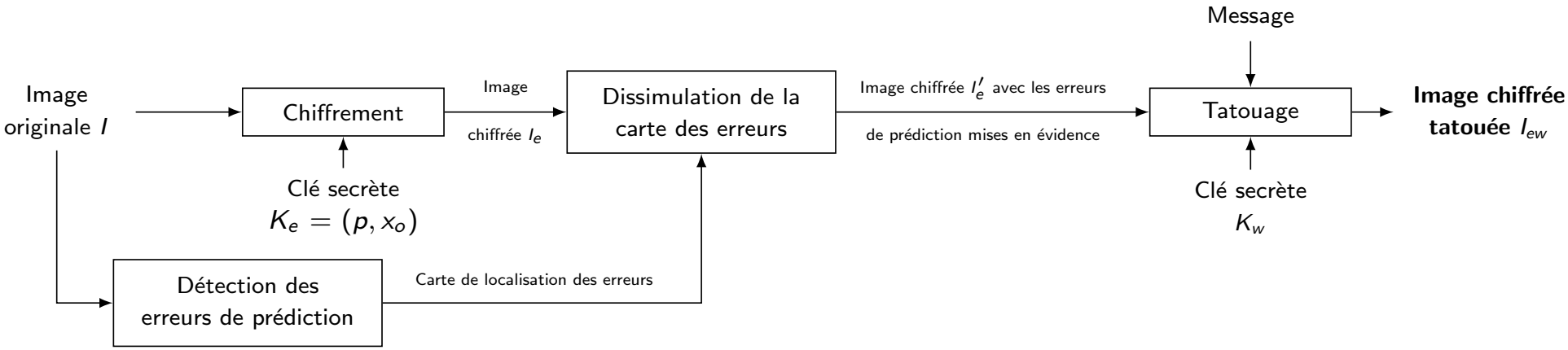


FIGURE – Chiffrement et tatouage

Localisation des erreurs de prédiction

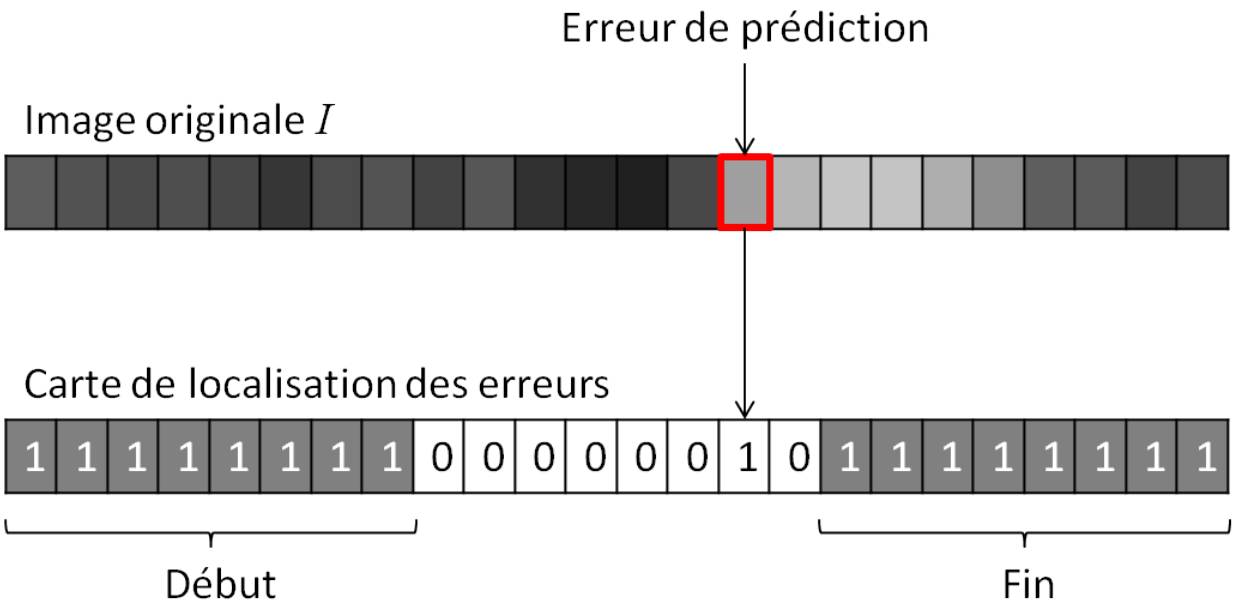


FIGURE – Construction de la carte de localisation des erreurs

Approche totalement réversible - Schéma général (2)

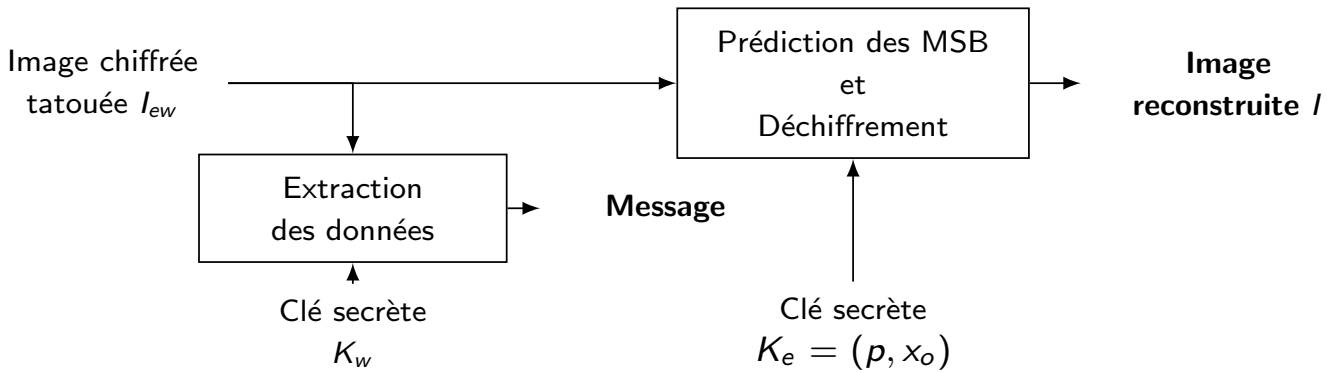


FIGURE – Extraction et reconstruction

Approche totalement réversible - Résultats

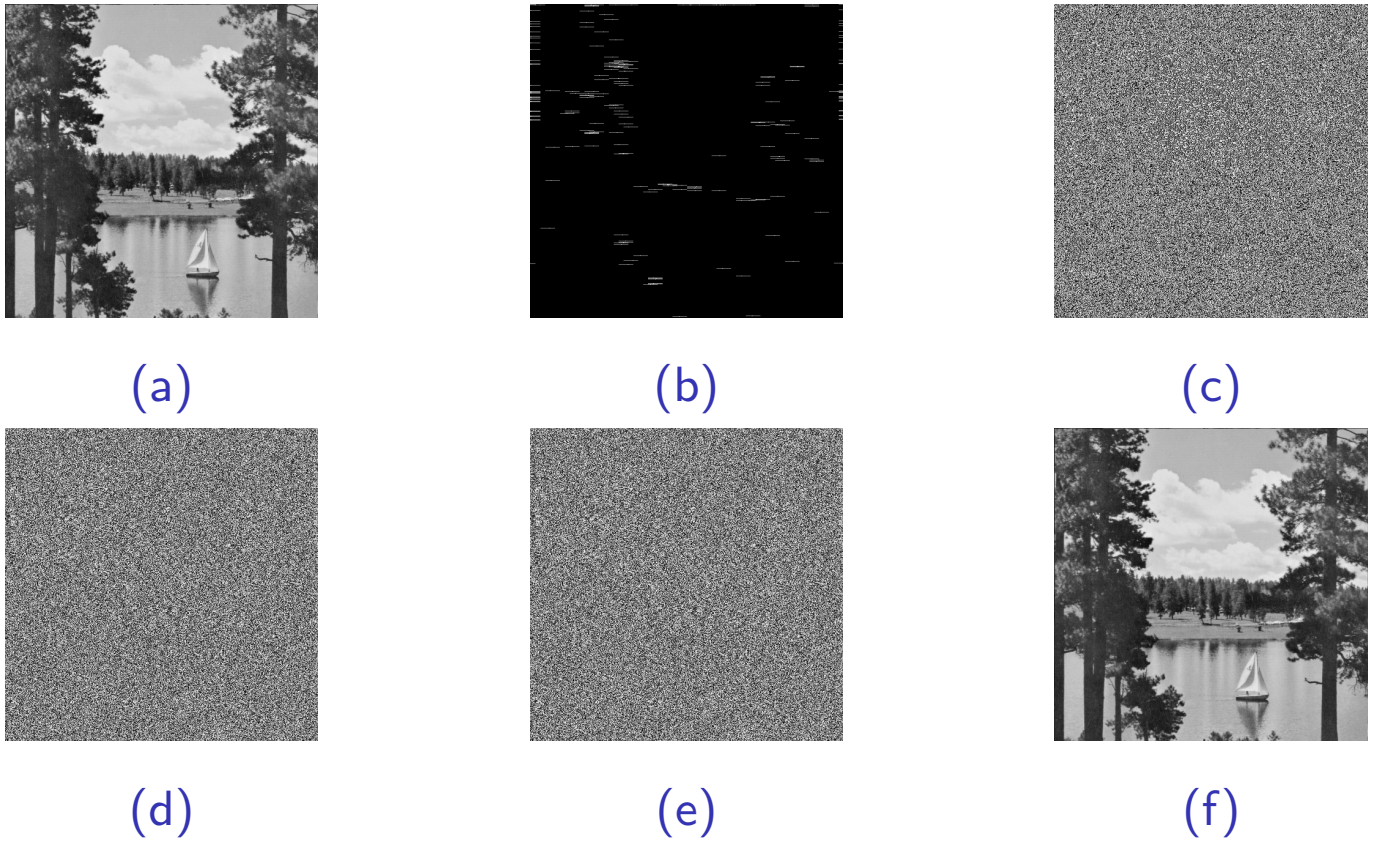


FIGURE – Illustration de notre méthode. a) Image originale I, b) Emplacement des pixels non tatoués (erreurs et drapeaux), nombre d'erreurs = 202 (0.1%), c) Image chiffrée I_e, d) Image chiffrée I'_e avec les erreurs de prédictions mises en évidence, e) Image chiffrée tatouée I_{ew}, payload = 0.9839 bpp, f) Image reconstruite I, PSNR = ∞, SSIM = 1

Approche totalement réversible - Résultats

	Meilleur cas	Pire cas	Moyenne
Nombre d'erreurs de prédiction des MSB dans l'image originale	0%	5.3%	0.2%
Payload (bpp)	1	0.3805	0.9681

TABLE – Mesures de la capacité de dissimulation sur une base de 10.000 images

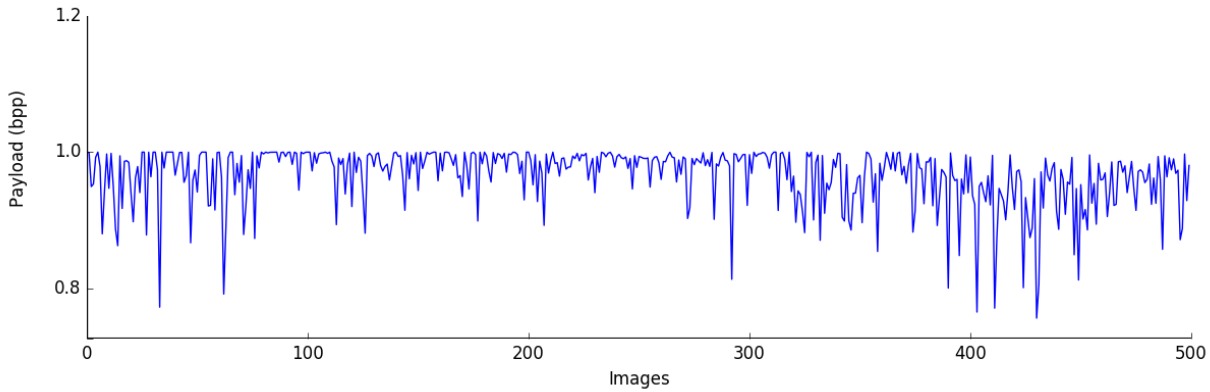


FIGURE – Mesures sur un échantillon de 500 images

Comparaison des deux méthodes avec la littérature

Images	Méthodes	Payload (bpp)	PSNR (dB)
Lena	Méthode 1	**1**	48.67
		0.5	52.08
		0.1667	57.58
	Méthode 2	0.96	$+\infty$
	Zhang	0.1563	44.65
	Wu et Sun	0.1563	$+\infty$
Baboon	Méthode 1	**1**	39.41
		0.5	44.00
		0.1667	48.82
	Méthode 2	0.75	$+\infty$
	Zhang	0.1563	38.79
	Wu et Sun	0.1563	40.57
Airplane	Méthode 1	**1**	57.24
		0.5	60.88
		0.1667	64.55
	Méthode 2	0.99	$+\infty$
	Zhang	0.1563	42.08
	Wu et Sun	0.1563	60.17

TABLE – Comparaison des performances entre la méthode de Zhang [1], celle de Wu et Sun [2] et les méthodes proposées

[1] X. Zhang
Separable reversible data hiding in encrypted images
IEEE Transactions on Information Forensics and Security, vol. 7(2), p.826-832, 2012

[2] X. Wu et W. Sun
High-capacity Reversible Data Hiding in Encrypted Images by Prediction Error
Signal Processing, vol. 104, p.387-400, 2014

Conclusion

Bilan des méthodes proposées

- **Approche 1** : Tatouage très haute capacité (payload ≥ 1 bpp) et bonne qualité de l'image reconstruite (haut PSNR)
- **Approche 2** : Image parfaitement reconstruite (PSNR $= \infty$) et haute capacité de dissimulation (payload ≈ 1 bpp)
- **Dans les deux cas** : Meilleurs résultats que dans la littérature

Perspectives

- **Approche 1** : Optimiser le choix du prédicteur utilisé pour avoir moins d'erreurs et/ou devoir effectuer de plus faibles modifications des valeurs des pixels
- **Approche 2** : Résoudre le problème de mauvaise détection des drapeaux
- **But final** : Trouver une méthode totalement réversible, avec un taux de dissimulation supérieur à 1 bpp

Merci pour votre attention !

Des questions ?