View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by HAL-Université de Bretagne Occidentale

International Journal of Computer Applications (0975 – 8887)
Volume 94 – No. 19, May 2014

A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key

Quist-Aphetsi Kester[124], Laurent Nana[2], Anca Christine Pascu[3], Sophie Gire[2], Jojo M. Eghan[4], and Nii Narku Quaynor[4]

[1]Faculty of Informatics, Ghana Technology University College, Accra, Ghana
[2]Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
[3]HCTI EA 4249 and Lab-STICC (UMR CNRS 6285) European University of Brittany, UBO, France
[4]Department of Computer Science and Information Technology, University of Cape Coast, Cape Coast, Ghana

ABSTRACT
The high increase in the transmission of digital data over secured and unsecured communications channels poses a lot of security and privacy concerns to both the transmitter and the receiver. Many operations engaged today in urban and warfare, be they for construction, monitory of plants, high voltage lines, military, police, fire service, intelligence etc. engages the use of surveillance systems that transmit sensitive data to and fro the command centre to the remote areas and this data in transmission needs to be secured. In this paper, we proposed a hybrid cryptographic and digital watermarking technique for securing digital images based on a Generated Symmetric Key. The cryptographic encryption technique made use of both pixel displacement and pixel encryption in securing the images that are to be stored or transmitted across secured and unsecured communications. The digital watermarking technique was used to authenticate the image. The programming and implementation was done using MATLAB.

General Terms
Cryptology, Symmetric Key, Algorithm, Security Digital image

Keywords
Cryptography, simulation, watermarking, digital image, RGB pixel shuffling

1. INTRODUCTION
The rapid continuous increase in exchange of multimedia data over protected and unprotected networks such as the worldwide available internet and local networks such as shared networks and local area networks etc has encouraged activities such as unauthorized access, illegal usage, disruption, alteration of transmitted and stored data.[1] This widely spread use of digital media over the internet such as on social media, won cloud storage systems etc and over other communication medium such as satellite communication systems have increased as applications and need for systems to meet current and future demands evolved over the years [2]. Security concerns with regards to such data transmission and storage has been a major concern of both the transmitters and receivers and hence the security of critical cyber and physical infrastructures as well as their underlying computing and communication architectures and systems becomes a very crucial priority of every institution [3].

Watermarking is a major image processing application used to authenticate user documents during transmission and storage by embedding and hiding some authenticated piece of information behind the digital data such as an image, audio or the video file [4]. The approaches engaged in the watermarking process can be visible or not based on the data format used and the watermarking approach. This hidden information is then used to verify the source or the authenticity of the transmitted data. Hence water marking plays a very important role in ownership verification when it comes to copyright issues, ownership of documents, etc for audio, video and other file formats. Cryptosystems engages different techniques in transforming a message to conceal its meaning and biometric cryptosystems have recently evolved as a means for solving key management issues as well as protecting biometric templates and a combination of cryptography and watermarking has helped in increasing the security in them[5].

Cryptography is the fundamental platform in which modern information security, which involves the use of advanced mathematical approaches in solving hard cryptographic issues, has gained its grounds in the digital world [6]. This has evolved from classical symmetric, in which shifting keys are normally used as well as substitution methods, [7][8] ciphers to modern public key exchange cryptosystems , which aims to make cryptanalysis a difficult approach to deciphering ciphers, [9][10] eg. RSA, ElGamal, elliptic curve, Diffie-Hellman key exchange[11][12][13], and they are used in digital signature algorithms and now cutting edge works such as the quantum cryptography [14][15].

The combination of both cryptographic and watermarking techniques can provide some important solutions for securing digital images. This hybrid approach will provide more solid grounds for an effective security of digital images.

This paper, we proposed a hybrid cryptographic and digital watermarking technique for securing digital images based on a Generated Symmetric Key. The cryptographic encryption technique made use of both digital image pixel displacement and visual cryptographic encryption techniques in securing the digital images engaged in the process. The digital watermarking technique was used to authenticate the image. The paper has the following structure: section II Related works, section III Methodology, section IV The mathematical explanation of the algorithm, section V results and analysis, and section VI concluded the paper.

2. RELATED WORKS

Digital watermarking and cryptography has strengthened the level of security in the transmission of data over secured and unsecured communication channels. Digital watermarking technique is commonly used to protect documents posted on the Internet etc. in recent years, the launching of social networking websites has highlighted the importance of looking into digital content security [16]. The rapid growth of the Internet has made copyright protection of digital contents a critical issue when it comes to ownership and distribution of such contents. A Digital Rights Management (DRM) system is aimed at protecting the high-value digital assets and controlling the distribution and utilization of those digital assets. Watermarking technologies are being regarded as a vital mean to proffer copyright protection of digital images. Digital watermarking hides, in digital images, the information necessary for ownership identity to offer copyright protection. Dorairangaswamy, M. A. and Padhmavathi, B. proposed an innovative invisible and blind watermarking scheme for copyright protection of digital images with the purpose of defending against digital piracy [17].In these days, people are using social networking media sites for sharing their life moments as images over the internet. And another side other users can access these images and use them on other sites for dubious and other means without the appropriate approval of the rightful owner or even download those digital images. A person can also exploits by editing and modifying the original image for other purposes. Modified images can then be uploaded and shared on other sites. The illegal use of personal image comes under copyright law. To address the stated issues Bhargava, N., Sharma, M.M., Garhwal, A.S. and Mathuria, M. in their work introduced a prototype for Digital Image Authentication System (DIAS). This system can perform visible and invisible watermarking on image. DIAS was applicable for color and gray images. The input image could be of any size, and the resultant image size would be same as input image. DIAS identified the ownership of digital image using Digital Watermarking. The Digital watermarking concept was used to hide and detect information from image. In their approach, digital watermarking was performed using Discrete Wavelet Transform (DWT)[18].

Both watermarking and cryptography have been used to authenticate and encrypt data. Digital watermarking is a promising technology to embed information as unperceivable signals in digital contents [19]. Shing-Chi Cheung, Dickson K. W. Chiu, and Cedric Ho proposed a watermark-based document distribution protocol, which complements conventional cryptography-based access control schemes; to address the problem of tracing unauthorized distribution of sensitive intelligence documents. They made use of intelligence user certificates to embed the identity of the users into the intelligence documents.

The large number of digital data and their circulation over different kinds of communication channels such as the internet with specific example like the social networks are making the copyright protection a very important issue in the digital world. This has resulted in the use of different watermarking techniques and visual cryptographic schemes for the copyright protection of digital images [20]. The combination of both techniques have provided some important solutions for tampering verification [21][22] and the resolution of disputes on the ownership of a given image, as provided by several proposals appeared in literature [23].

Singh, T.R., Singh, K.M., and Roy, S., proposed a robust video watermarking scheme based on visual cryptography. They used different parts of a single watermark as different scenes of a video for generation of the owner's share from the original video based on the frame mean in same scene and the binary watermark, and generation of the identification share based on the frame mean of probably attacked video [24].

Fallahpour, M., Shirmohammadi, S., Semsarzadeh, M. and Zhao, J., presented a method to detect video tampering and distinguished it from common video processing operations, such as recompression, noise, and brightness increase, using a practical watermarking scheme for real-time authentication of digital video. In their approach, the watermark signals represented the macro block's and frame's indices, and were embedded into the nonzero quantized discrete cosine transform value of blocks, mostly the last nonzero values, enabling their method to detect spatial, temporal, and spatiotemporal tampering and their approach took advantage of content-based cryptography and increases the security of the system[25].

Robustness has become a common practice in most of the digital image watermarking schemes; it becomes a common practice to address security. Such consideration in developing and evaluation of a watermarking scheme may severely affect the performance and render the scheme ultimately unusable [26]. Robustness, even if recognized as a key property of the digital watermarking, is not considered enough to prove the ownership of images [27] but rather test the watermarking algorithm against various types of attacks [28]. The dual implementation of watermarking and visual cryptography enhances the security strength and reliability of transmitted image data over communication channels [29][30].

In our work we proposed a cryptographic encryption technique that made use of both pixel displacement and encryption in securing the images based on a generated symmetric key. The digital watermarking technique was used to authenticate the image.

3. METHODOLOGY

Watermarking is generally used to embed "secret" information into an original digital data in a form of audio, images etc. This is used to verify the authenticity of the digital image. The approaches of the watermarking can be visible or invisible after its implementation. Visual cryptography encryption technique refers to a way to decompose a secret image into n numbers of shares and distribute them to a number of participants, so that only legitimate subsets of participants can reconstruct the original image by combining their n shares [31].

In This paper, we proposed hybrid cryptographic and digital watermarking technique for securing digital images based on a generated symmetric key from the image features. The watermarking approach engaged a sequential embedding technique and the method was then used in the authentication process of the image at the pixel level. The resulted ciphered image was then encrypted using pixel displacement algorithm based on the generated key.

The analysis of the results clearly showed that the total no of pixels of the images, both plain and ciphered, at the end of the encryption and the decryption process experienced a pixel loss that was insignificant to the quality change in the watermarked image. The original image was obtained from the ciphered image by decrypting it as well as removing the watermarking. This approach is effective when it comes to the transmission of digital images that needs to be verified at each node of the transmission system. The proposed method of the

cryptographic and the watermarking process were implemented on nxm size of images which proved to be very effective at the end. The implementation and the analysis of the images were done using MATLAB. The figure 1 below is the summary of the cryptographic and watermarking technique used in the encryption process of the digital plain image. Where PI is the plain image and CI is the ciphered image. Alg(PI,β,α) is the algorithm used in the embedding of the watermark and ciphering process.

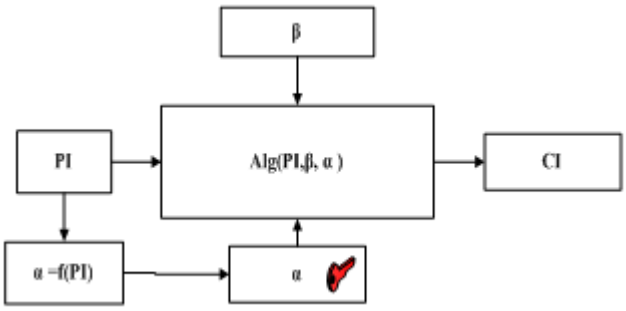


Fig 1: The summary of the processes engaged.

B=message embedded

α =symmetric encryption key for the pixel encryption.

f(PI)=symmetric key generated from the plain image.

4. THE MATHEMATICAL EXPLANATION

The processes engaged in the watermarking and the cryptography which involves the RGB pixel shuffling and displacement algorithm are explained below.

4.1 Implementation of the Watermarking

Watermarking is a method used to embed "secret" information into an original image by engaging different approaches. This can be visually identified on the images or not. The following method was used to embed the data into the plain image using MATLAB.

Step1. Start

Step2. Reading the various RGB color composition of the plain image data,

Let PI= f (R, G, B)

new_image=imread(PI);

PI is a color image of m x n x 3 arrays

$$\begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \end{pmatrix}$$

(R, G, B) = m x n

Where R, G, B ∈PI

(R o G) i j = (R) ij. (G) ij

Where r_11 = first value of R

r= [ri1] (i=1, 2… m)

x ∈ r_i1 : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

R= r= I (m, n, 1)

Where g_12 = first value of G

g= [gi2] (i=1, 2... m)

x ∈ g : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

G= g= I (m, n, 1)

And b_13 = first value of B

g= [bi3] (i=1, 2... m)

x ∈ b_i1 : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

B=b= I (m, n, 1

Such that R= r= I (m, n, 1)

Step3. R=f (:,:,1);

Extraction of the red component as 'r' from the plain image

Let (:,:,1)=size of R be m x n [row, column] = size (R) = R (m x n)

rij= r= I (m, n, 1) =

$$\begin{pmatrix} R \\ r_{i1} \\ \vdots \\ r_{in} \end{pmatrix}$$

Step4. g=f (:,:,2);

Extraction of the green component as 'g' from the plain image

Let (:,:,2)=size of G be m x n [row, column] = size (G)

gij= g= I (m, n, 1) =

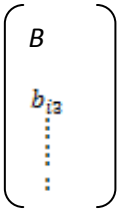
$$\begin{pmatrix} G \\ g_{i2} \\ \vdots \\ g_{n2} \end{pmatrix}$$

Step5. b=f (:,:,3);

Extraction of the blue component as 'b' from the plain image

Let f (:,:,3);=ize of B be m x n [row, column] = size (B) = B (m x n)

bij= b= I (m, n, 1) =



Step6. [c, p]=s(r);

Let the size of r as [c, p]

Let s(r) =size of R be [row, column] = size (r) =r (c x p)

Step7. Embedding the data into the plain image PI

d=Aij, where d is the data to be embedded into the plain image

Let the size of d be [c1, p1]=size(d);

Let λ=xi : x i∈ I: 0 ≤ x ≥ ∞;

Let η=xi : x i∈ I: 0 ≤ x ≥ ∞;

for i=1:1:c1

for j=1:1:p1

if((i== λ)&& (j== η))

t(i,j)= Aij;

y(i,j)=g(i,j);

u(i,j)=b(i,j);

λ = λ +Δ λ ;

η = η +Δ η ;

if(c1<c)

t(i,j)=r(i,j);

y(i,j)=g(i,j);

u(i,j)=b(i,j);

if(p1<p)

t(i,j)=r(i,j);

y(i,j)=g(i,j);

u(i,j)=b(i,j);

else

end

else

t(i,j)=r(i,j);

y(i,j)=g(i,j);

u(i,j)=b(i,j);

end

end

end

4.2 The Symmetric key generation process

The generation of the symmetric key was performed on the plain image based on certain features of the image as follows:

Let the set of bits positions in X be x: x∈ X and X→ x: x=xi = [x0, x1, x2, x3… xn] and x ∈ I where I is a positive integer.

SSK=$\sum_{k=1}^{n} \Psi_k$ Where $\Psi_k$is the decimal value of xi

Sk = [3*(c x p)+| (δ x 103)| +| (gm= 2*(1/n) .∑ni=1xi)|] mod p

K= (Sk.SSK) mod p Where p∈ I, δ= Entropy of image

ε = Gray value of an input image (0-255).

Ψ (η) = Probability of the occurrence of symbol η

gm is the arithmetic mean for all the pixels in the image

Where K is the key obtained

4.3 The image encryption process

The process used in the image encryption with the engagement of the key in the ciphering of the image and displacing the pixel values is shown below:

Engagement of K in the encryption of the plain image.

for i: Δi:K

Let t'(i,j) =Transpose of t(i,j)

t'(i,j)= f(r',c,p);

Let y'(i,j) =Transpose of y(i,j)

y'(i,j)= f(g',c,p);

Let u'(i,j) =Transpose of u(i,j)

u'(i,j)= f(b',c,p);

end

Transformion of t'(i,j) into f(t'(i,j),c,p))

r= f(t'(i,j),c,p))=f(r, c, p)

Transformion of y'(i,j)into f(y'(i,j),c,p))

g= f(y'(i,j),c,p))=f(g, c, p)

Transformion of u'(i,j) into f(u'(i,j),c,p))

b= f(u(i,j),c,p))=f(b, c, p)

CI= f (3,r,g,b);

end

5. SIMULATED RESULTS AND ANALYSIS

The image below was captured using a surveillance camera and four frames have been encrypted analyzed using the algorithm which was implemented in MATLAB.

Fig 2 The (1824 x 1018 pixel image) plain image used.

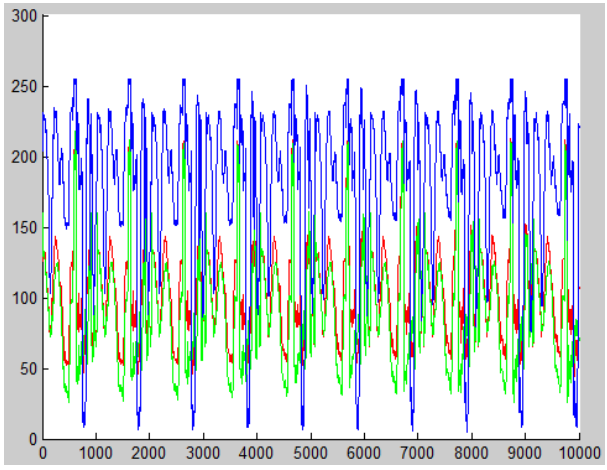


Fig 3: The first 10000 pixel value of the plain image.

Fig 4: The watermarked image.

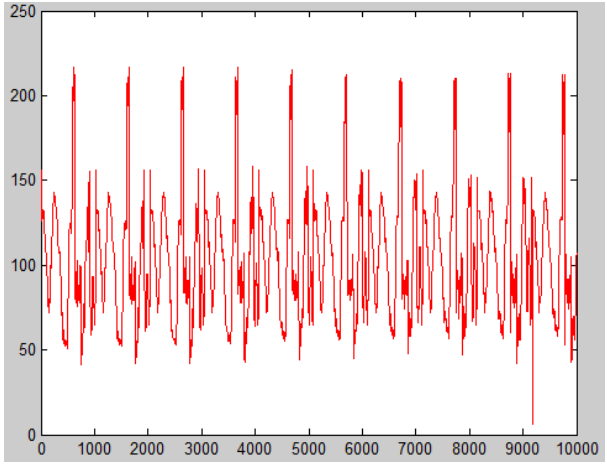


Fig 5: The first 10000 R pixel values of the watermarked image.

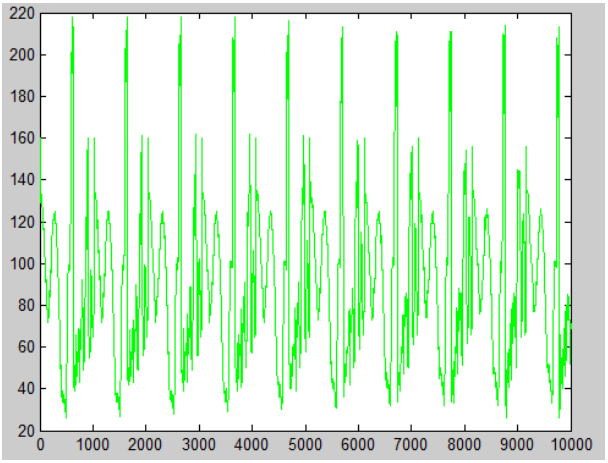


Fig 6: The first 10000 G pixel values of the watermarked image.

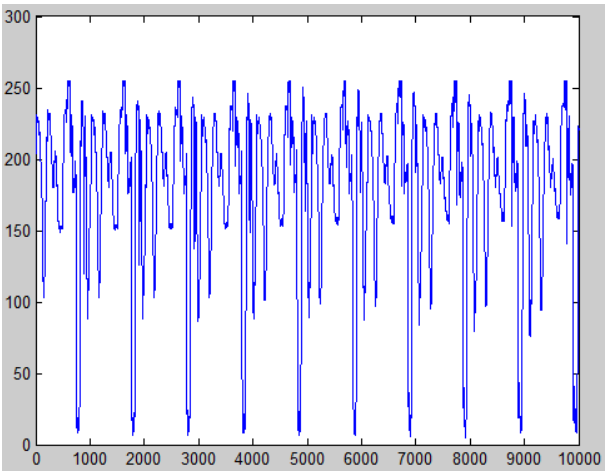


Fig 7: The first 10000 b pixel values off the watermarked image

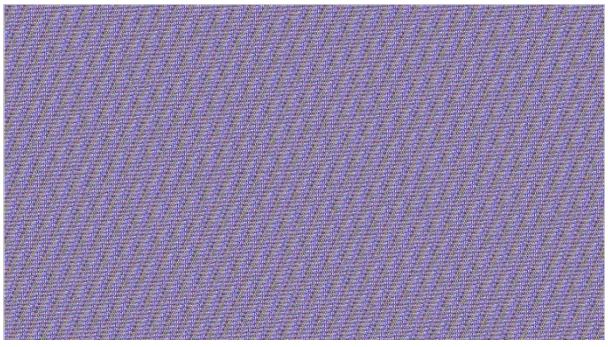


Fig 4: The ciphered image-watermarked image.

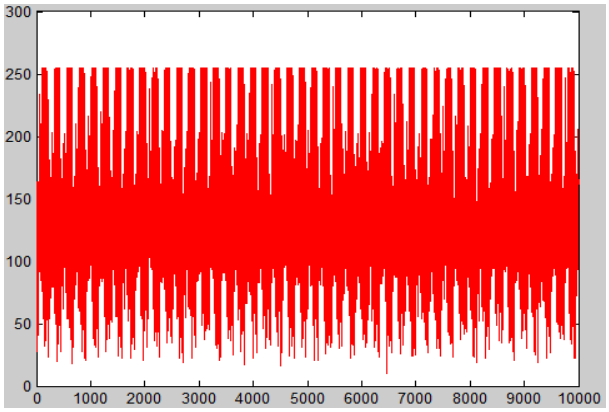


Fig 9:The first 10000 R pixel values of the ciphered image.

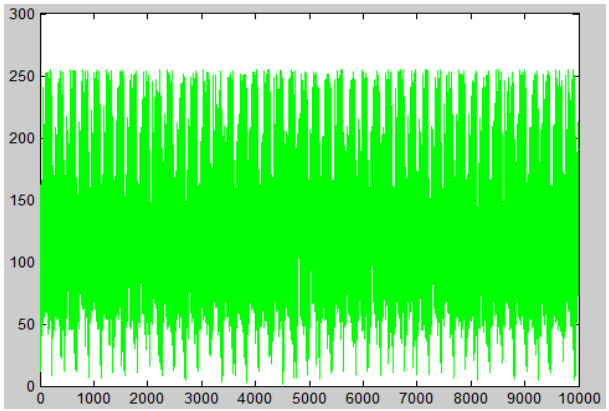


Fig 10: The first 10000 G pixel values of the ciphered image-watermarked image.

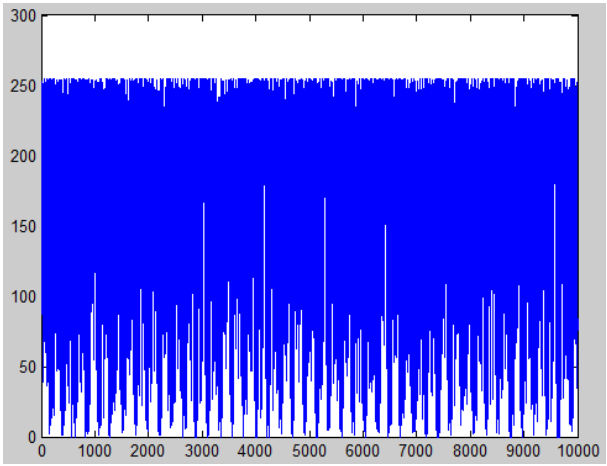


Fig 11: The first 10000 B pixel values of the ciphered image-watermarked image.

The plain image in figure 2 above is the mxn image used for the analysis with its first 10000 pixel values plotted in figure 3. Figure 4 represented the watermarked image and its first 10000 R, G, B pixel values were plotted in figure 5,6 and 7 respectfully. Figure 8 is the result of the ciphered image and its first 10000 R, G, B pixel values were plotted in figure 9, 10 and 11 respectfully

m = geomean(xi). It calculates the geometric mean of a the plain, watermarked and ciphered images.

The geometric mean is

$$m = \left[\prod_{i=1}^{n} xi\right]^{\frac{1}{n}}$$

δ(xi) = entropy(I) returns the Entropy of the plain, watermarked and ciphered images, which is a scalar value representing the entropy of grayscale image I. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.

Entropy is defined as δ(i))=-sum(xi.*log2(xi))

Ÿ(xi) returs the index value of the geometric mean of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image.

$$Ÿ(xi) = m(xi) / \Sigma((xi=\{R,G,B\}))$$

Ψ (xi) returs the index value of the entropy of the plain, watermarked and ciphered images with respect to the total entropy of the RGB image.

$$\Psi(xi) = \delta(xi) / \Sigma((xi=\{R,G,B\}))$$

Table 1. Analysis of plain, watermarked and cipherd image.

xi	*m*	δ(xi)	Ÿ(xi)	Ψ (xi)
PI(R)	141.6829	7.5739	0.3239	0.32858
PI(G)	128.1459	7.7500	0.2929	0.33622
PI(B)	167.6185	7.7268	0.3832	0.33521
WI(R)	141.6758	7.5744	0.0173	0.00003
WI(G)	128.1459	7.7500	0.0177	0.00003
WI(B)	167.6185	7.7268	0.0177	0.00003
CI(R)	141.6758	7.5744	0.3239	0.32859
CI(G)	128.1459	7.7500	0.2929	0.33621
CI(B)	167.6185	7.7268	0.3832	0.33520

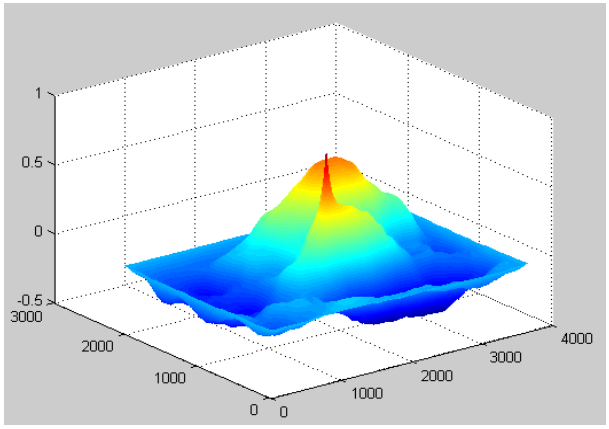


Fig 12: The graph of the normalized cross-correlation of the matrices of the plain image.

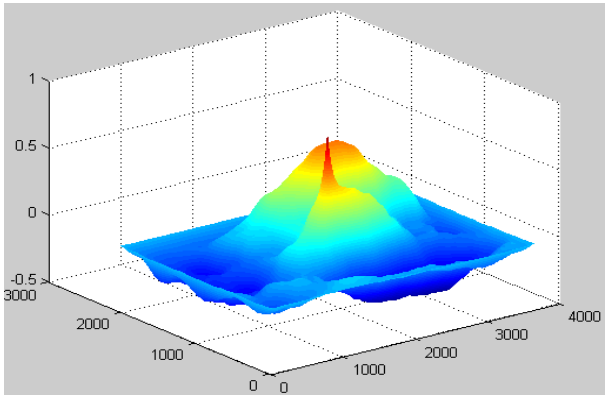


Fig 13: The graph of the normalized cross-correlation of the matrices of the plain image.

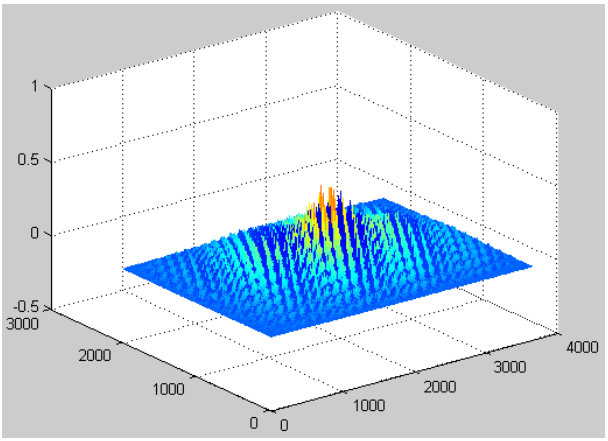


Fig 12: The graph of the normalized cross-correlation of the matrices of the ciphered image

The normalized cross-correlation of the matrices of is

$$\gamma(u,v)=\frac{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]\left[t(x-u,y-v)-\bar{t}\right]}{\left\{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]^2\sum_{x,y}\left[t(x-u,y-v)-\bar{t}\right]^2\right\}^{0.5}}$$

f is the mean of the template

t is the mean of in the region under the template.

f (u,v) bar, is the mean of $f(u,v)$ in the region under the template.

6. CONCLUSION

The hybrid nature of the procedure involving both the watermarking and cryptographic method proved to be successful. Even though there was a non-significance pixel loss aspect of the process the quality of the image was good.

The entropy values and the mean values of the image for the plain, watermarked and the ciphered image remained approximately the same.

7. ACKNOWLEDGMENTS

This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientic counselor of AWBC..

8. REFERENCES

[1] Musheer Ahmad and Tanvir Ahmad. 2014. Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys. Int. J. Commun. Netw. Distrib. Syst. 12, 1 (November 2014), 113-128. DOI=10.1504/IJCNDS.2014.057991http://dx.doi.org/ 10.15 04/I J CNDS.2014.057991

[2] Jonathan Bishop. 2014. Representations of 'trolls' in mass media communication: a review of media-texts and moral panics relating to 'internet trolling'. Int. J. Web Based Communities 10, 1 (December 2014), 7-24.

DOI=10.1504/IJWBC.2014.058384 http://dx.doi.org/ 10.1504/IJWBC.2014.058384

[3] Sajal K. Das, Krishna Kant, and Nan Zhang. 2012. Handbook on Securing Cyber-Physical Critical Infrastructure (1st ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[4] Kumar, M.; Hensman, A., "Robust digital video watermarking using reversible data hiding and visual cryptography," Signals and Systems Conference (ISSC 2013), 24th IET Irish , vol., no., pp.1,6, 20-21 June 2013 doi: 10.1049/ic.2013.0051

[5] Fouad, M.; El Saddik, A.; Jiying Zhao; Petriu, E., "Combining cryptography and watermarking to secure revocable iris templates," Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE , vol., no., pp.1,4, 10-12 May 2011doi: 10.1109/IMTC.2011.5944015

[6] Song Y. Yan. 2013. Computational Number Theory and Modern Cryptography (1st ed.). Wiley Publishing.

[7] Toorani, M.; Falahati, A., "A secure variant of the Hill Cipher," Computers and Communications, 2009. ISCC 2009. IEEE Symposium on , vol., no., pp.313,316, 5-8 July 2009doi: 10.1109/ISCC.2009.5202241

[8] Minglei Zha; Bin Wang, "On the fast algebraic immunity of even-variable rotation symmetric Boolean functions," Advanced Communication Technology (ICACT), 2012 14th International Conference on , vol., no., pp.221,224, 19-22 Feb. 2012

[9] Saeed, Q.; Basir, T.; Ul Haq, S.; Zia, N.; Paracha, M.A., "Mathematical Hard Problems in Modern Public-Key Cryptosystem," Emerging Technologies, 2006. ICET '06. International Conference on , vol., no., pp.456,460, 13-14 Nov. 2006 doi: 10.1109/ICET.2006 .335986

[10] Anand, D.; Khemchandani, V.; Sharma, R.K., "Identity-Based Cryptography Techniques and Applications (A Review)," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.343,348, 27-29 Sept. 2013 doi: 10.1109/CICN.2013.78

[11] Burton S. Kaliski, Jr.. 1996. IEEE P1363: A Standard for RSA, Diffie-Hellman, and Elliptic-Curve Cryptography (Abstract). In Proceedings of the International Workshop on Security Protocols, T. Mark A. Lomas (Ed.). Springer-Verlag, London, UK, UK, 117-118.

[12] Lo'ai A. Tawalbeh and Saadeh Sweidan. 2010. Hardware Design and Implementation of ElGamal Public-Key Cryptography Algorithm. Inf. Sec. J.: A Global Perspective 19, 5 (January 2010), 243-252. DOI=10.1080/19393555.2010.499799 http://dx.doi.org/10.1080/19393555.2010.499799

[13] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. 2007. Provably secure authenticated group Diffie-Hellman key exchange. ACM Trans. Inf. Syst. Secur. 10, 3, Article 10 (July 2007). DOI=10.1145/1266977.1266979 http://doi.acm.org/10.1145/1266977. 1266979

[14] Kester, Q.-A.; Nana, L.; Pascu, A.C., "A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications," Adaptive Science and Technology (ICAST), 2013 International Conference on , vol., no., pp.1,6, 25-27 Nov. 2013 doi: 10.1109/ICASTech.2013.6707496

[15] Chip Elliott, David Pearson, and Gregory Troxel. 2003. Quantum cryptography in practice. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03). ACM, New York, NY, USA, 227-238. DOI=10.1145/863955.863982 http://doi.acm.org/10.1145/86395 5. 863982

[16] Wei-Fan Hsieh; Pei-Yu Lin, "Analyze the Digital Watermarking Security Demands for the Facebook Website," Genetic and Evolutionary Computing (ICGEC), 2012 Sixth International Conference on , vol., no., pp.31,34, 25-28 Aug. 2012 doi: 10.1109/ICGEC.2012.62

[17] Dorairangaswamy, M. A.; Padhmavathi, B., "An effective blind watermarking scheme for protecting rightful ownership of digital images," TENCON 2009 - 2009 IEEE Region 10 Conference , vol., no., pp.1,6, 23-26 Jan. 2009doi: 10.1109/TENCON.2009.5395812

[18] Bhargava, N.; Sharma, M.M.; Garhwal, A.S.; Mathuria, M., "Digital image authentication system based on digital watermarking," Radar, Communication and Computing (ICRCC), 2012 International Conference on , vol., no., pp.185,189, 21-22 Dec. 2012 doi: 10.1109/ICRCC.2012.6450573

[19] Shing-Chi Cheung, Dickson K. W. Chiu, and Cedric Ho. 2008. The use of digital watermarking for intelligence multimedia document distribution. J. Theor. Appl. Electron. Commer. Res. 3, 3 (December 2008), 103-118.

[20] Stelvio Cimato, James Ching-Nung Yang, and Chih-Cheng Wu. 2012. Visual cryptography based watermarking: definition and meaning. In Proceedings of the 11th international conference on Digital Forensics and Watermaking (IWDW'12), Yun Q. Shi, Hyoung-Joong Kim, and Fernando Pérez-González (Eds.). Springer-Verlag, Berlin, Heidelberg, 435-448. DOI=10.1007/978-3-642-40099-5_36 http://dx.doi.org/10.1007/978-3-642-40099-5_36

[21] I-Kuan Kong and Chi-Man Pun. 2008. Digital Image Watermarking with Blind Detection for Copyright Verification. In Proceedings of the 2008 Congress on Image and Signal Processing, Vol. 1 - Volume 01 (CISP '08), Vol. 1. IEEE Computer Society, Washington, DC, USA, 504-508. DOI=10.1109/CISP.2008.546 http://dx.doi.org/ 10.1109/CISP.2008.546

[22] Huiping Guo. 2003. Digital Image Watermarking for Ownership Verification. Ph.D. Dissertation. University of Ottawa, Ottawa, Ont., Canada, Canada. Advisor(s) Nicolas Georganas. AAINQ85364.

[23] Huaqing Liang, Hongdong Yin, and Xinxin Niu. 2009. A Robust Digital Watermarking Scheme and Its Application in Certificate Verification. In Proceedings of the 2009 International Conference on Measuring Technology and Mechatronics Automation - Volume 01 (ICMTMA '09), Vol. 1. IEEE Computer Society, Washington, DC, USA, 410-413. DOI=10.1109/ICMTMA.2009.295 http://dx.doi.org/10.1109/ICMTMA.2009.295

[24] Singh, T.R.; Singh, K.M.; Roy, S., "Robust video watermarking scheme based on visual cryptography," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.872,877, Oct. 30 2012-Nov. 2 2012 doi: 10.1109/WICT.2012.6409198

[25] Fallahpour, M.; Shirmohammadi, S.; Semsarzadeh, M.; Zhao, J., "Tampering Detection in Compressed Digital Video Using Watermarking," Instrumentation and Measurement, IEEE Transactions on , vol.63, no.5, pp.1057,1072, May 2014doi: 10.1109/TIM.2014.2299371

[26] Nyeem, H.; Boles, W.; Boyd, C., "On the robustness and security of digital image watermarking," Informatics, Electronics & Vision (ICIEV), 2012 International Conference on , vol., no., pp.1136,1141, 18-19 May 2012 doi: 10.1109/ICIEV.2012.6317496

[27] Gilani, J.; Mir, A.A., "Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques," Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. SNPD '09. 10th ACIS International Conference on , vol., no., pp.399,404, 27-29 May 2009 doi: 10.1109/SNPD.2009.89

[28] Kamel, I.; Al Koky, O.; Al Dakkak, A., "Distortion-Free Watermarking Scheme for Wireless Sensor Networks," Intelligent Networking and Collaborative Systems, 2009. INCOS '09. International Conference on , vol., no., pp.135,140, 4-6 Nov. 2009 doi: 10.1109/INCOS.2009.67

[29] Nassiri, B.; Latif, R.; Toumanari, A.; Maoulainine, F.M.R., "Secure transmission of medical images by watermarking technique," Complex Systems (ICCS), 2012 International Conference on , vol., no., pp.1,5, 5-6 Nov. 2012 doi: 10.1109/ICoCS.2012.6458577

[30] Daojing Li; Bo Zhang, "DWTC: A Dual Watermarking Scheme Based on Threshold Cryptography for Web Document," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.8, no., pp.V8-510,V8-514, 22-24 Oct. 2010 doi: 10.1109/ICCASM.2010.5620633

[31] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo Moses Eghan, Nii Narku Quaynor. A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images. International Conference on Systems Informatics, Modelling and Simulation. pp.1-6. IEEE. SIMS2014.