A New Cryptographic Encryption Algorithm for Securing Digital Images

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
This paper proposed a new algorithm for digital image encryption. The proposed algorithm encrypts an mxn size image by using the set of array pixel values. At the end, plain images will be encrypted using the algorithm and analysis will be performed on the ciphered images to determine the efficiency of the algorithm in ciphering the image. The algorithm ultimately makes it possible for encryption and decryption of the images to be done based on the RGB pixel. The algorithm was implemented using MATLAB.

General Terms
Cryptology, Encryption, Algorithm, Security Digital image

Keywords
Pixel displacement, encryption, RGB, Cryptography

1. INTRODUCTION
In today's cyberspace where there exists several security challenges associated with the processing and transmission of digital images over an open and unsecured network. These challenges pose a lot of debate on privacy and security of transmitted data. There exists a high concern of insecurity due to malicious activities over these open networks. It is therefore necessary to assure the confidentiality, the integrity and the authenticity of the digital image transmission over these open and unsecured networks which modern day cryptography can provide.

In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The unreadable data which is the ciphered data have to be difficult or virtually impossible to decipher. The result of the process of making information unreadable in its state is known as encryption. The reverse process is referred to as decryption.[1] Cryptography has evolved from the from classical such as Caesar, Vigenère, Trifid ciphers to modern day cipher and public key systems such as Diffie-Hellman, RSA etc[2].With the rapid increase in the development of advanced network technology, multimedia information is transmitted openly over the Internet conveniently and encryption of such data is very crucial. Various confidential data such as, image data from unmanned Ariel vehicles, military maps and video from remote devices need to be secured. There have been a lot works done in pixel displacements at the software level [5] which have to do with internet multimedia applications and some implementations at the hardware level [6].

This research work proposed a new method of digital image encryption based on an algorithm that uses the RGB pixel values of the plain image for the encryption process.

The paper has the following structure: section II Related works, section III Methodology, section IV The algorithm, section V architectural summary of the encryption process using flowchart section VI results and analysis, and section VII concluded the paper..

2. RELATED WORKS
Cryptography has engaged advanced mathematical approaches over the years and it has strengthened the level of security in the transmission of data over secured and unsecured communication channels. Cryptography has been used to authenticate and encrypt data. There have also been specific works with image cryptography which involves both pixel and visual cryptographic techniques [7]. Maksuanpan, S. and San-Um, W., in their work proposed a cryptography technique that realizes a XOR operation between separated planes of binary gray-scale image and a shuffled multi-scroll DDE chaotic attractor image. Their security keys were parameters in DDE, with initial conditions, time constants, and simulation time that sets final states of an attractor. Their experimental results were performed in MATLAB [8]. Wu, Xiaoyu, Wong, Duncan S. and Li, Qing, worked on a k-out-of-n Extended Visual Cryptography Scheme (EVCS) which is a secret sharing scheme which hides a secret image into n shares, which are also some images. With this method the secret image can be recovered if at least k of the shares are superimposed, while nothing can be obtained if less than k shares are known. Previous EVCS schemes were either for black-and-white images or having pixel expansion. With their work, they proposed the first k-out-of-n EVCS for color images with no pixel expansion. Their scheme also improved the contrast of the n shares and the reconstructed secret image (i.e. the superimposed image of any k or more shares) by allowing users to specify the level of each primary color (i.e. Red, Green and Blue) in the image shares as well as the reconstructed secret image [9]. Visual cryptography, Askari, N., Heys, H.M. and Moloney, C.R., proposed a method for processing halftone images that improved the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image was the same as for the original halftone secret image. The resulting scheme maintained the perfect security of the original extended visual cryptography approach [10]. Monoth, T. and Babu, A.P., proposed schemes that achieved better contrast and reduced the noise in the reconstructed secret image without any

computational complexity. In their method, additional pixel patterns were used to improve the contrast of the reconstructed secret image [11].

3. METHODOLOGY

In this method, we proposed a technique for image encryption based on RGB pixel displacement. At the end of our encryption process, there was no change of the bit values and there were no pixel expansion at the end of the encryption and the decryption process. This means that, the total sum of all the pixels of the image remained unchanged as well as the respective pixel values. The image was decomposed based on three principle component by the algorithm. The images used have their RGB pixel values extracted and operated on by the proposed algorithm to obtain the ciphered image. The R-G-B components were considered as the triplet that formed the characteristics of a pixel of the images used. The ciphering of the image for this research was done by using the RBG pixel values of the images.

In the process, the RGB values were extracted, transposed, reshaped and as well as shifted out of its original pixel position by the algorithm and interchanged within the image boundaries by the algorithmic process represented in figure 1. The Shift displacement of the R G and B Values known termed as the component displacement factor array is different for R, G and B. The shifting effect is dependent on the number of iterations performed by the algorithm.

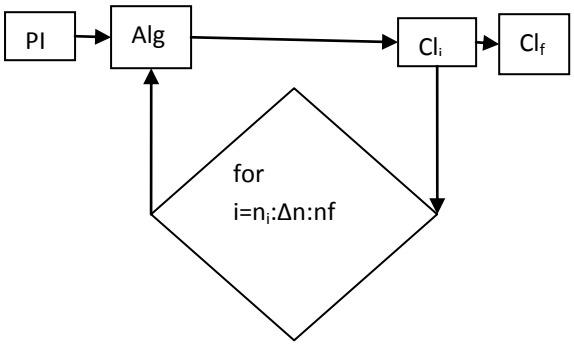

Fig 1: the encryption algorithm process

Where PI= plain Image, Alg=Algorithm, Cli=Initial ciphered image and CIf=Final ciphered image and i=ni:Δn:nf loops the encryption process from a minimum specified value of n to a maximum specified value of n with a change in n as the step and n is an integer.

With the proposed method in this paper, the encryption of the plain image will be solely done by using the RGB pixels values.

4. THE ALGORITHM

Start

Let Q= an image= Ψ (R, G, B) and Let PI=Q

Where R, G, B ∈ Q and (R o G)ij = (R) ij. (G) ij

Where R= ri1 = Qi1

r= [ri1] (i=1, 2… m)

x ∈ ri1 : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

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

Where G= gi2 = Qi2

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

x ∈ g : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

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

And B= bi3 = Qi3

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

x ∈ bi1 : [a, b]= {x ∈ I: a ≤ x ≥ b}

a=0 and b=255

B=b= Q (m, n, 1)

P.I=Ψ (3, Φ, Γ, Λ)

for i=ni:Δn:nf

Φ= Ψ (: , : , 1)

Γ= Ψ (: , : , 2)

Λ= Ψ (: , : , 3)

[β, γ]= [m, n] (Γ);

R = Φ `

G = Γ `

B = Λ `

r = Ω (R, β, γ)

g= Ω (G `, β, γ)

b =Ω (B `, β, γ)

Ei= Ψ (3, r, g, b)

Next i

Ef= Ψ (3, r, g, b)

Stop

The inverse of the algorithm will decrypt the encrypted image back into the plain image.

From the proposed algorithm, the plain image has a composition of RGB pixel values. The RGB values were then separated into their respective vector components. The red component of the image was then extracted and passed on to the variable 'Φ'. The green component of the image was then extracted and passed on to the variable 'Γ'. And the blue component of the image was then extracted and passed on to the variable 'Λ'. Φ, Γ and Λ were then transposed. The array values of the transposed pixels are then rearranged according to the dimension of β and γ. The respective values are then concatenated into an image data format and then passed on to the variable 'Ei'. The process is repeated until the number of iterations set up within the loon is satisfied. The implantation of the algorithm was done using MATLAB and the code was run to perform the ciphering of the plain images used in this paper. The ciphered images produced by the algorithm were analyzed in order to see its efficiency.

5. THE ARCHITECTURAL SUMMARY OF THE ENCRYPTION PROCESS USING FLOWCHART

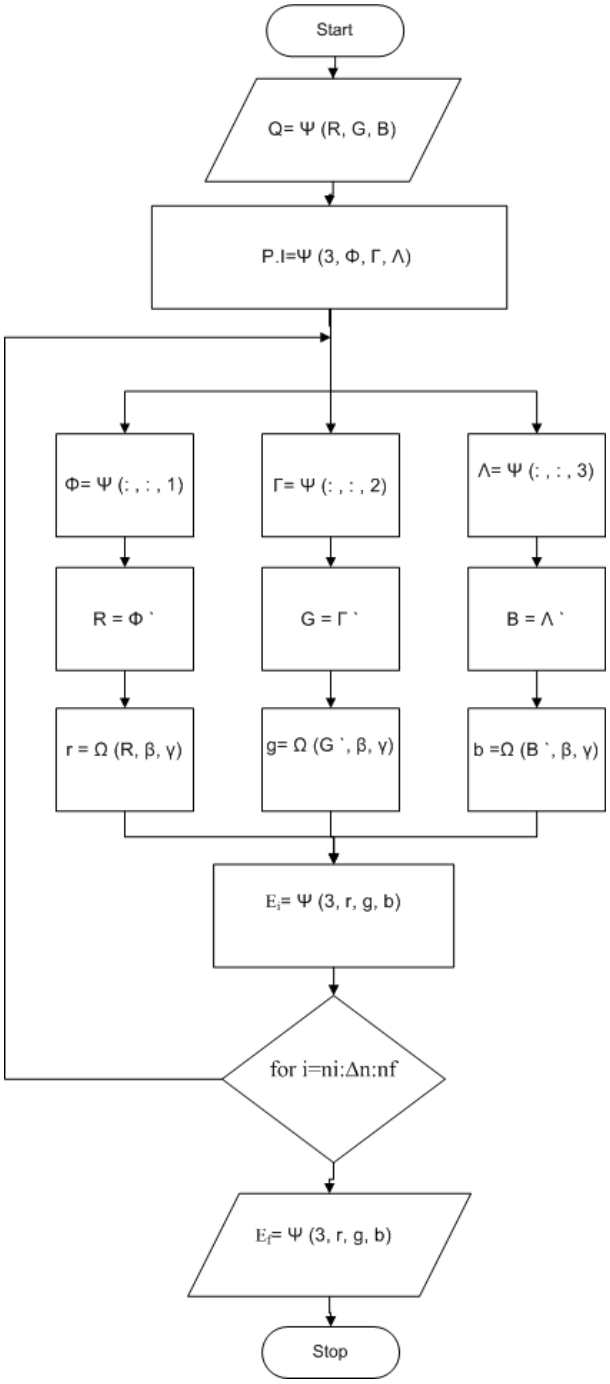

Fig 2: Flow chart diagram for the encryption algorithm

Figure 2 showed the summary of the encryption of the plain image and then figure 2 showed the flow chart diagram for the encryption and decryption process. It illustrates how the data is retrieved

6. RESULTS AND ANALYSIS

The implementation of the algorithm was done using MATLAB Version 7.12.0 (R2011a). The image sizes used was not fixed since the algorithm can work on mxn image size. The algorithm was written in m-file and tested with the output results shown below.

Fig 3: Plain image 1

Fig 4: Plain image 2

Fig 5: Plain image 3

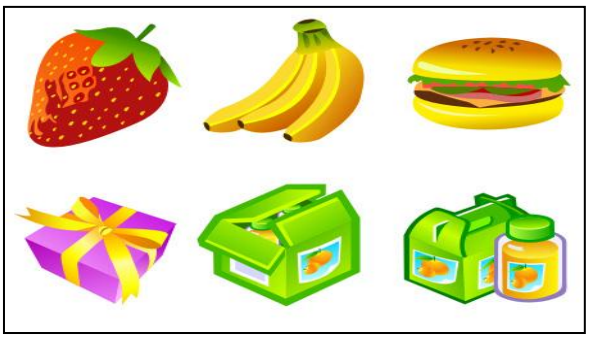

Fig 6: Plain image 4

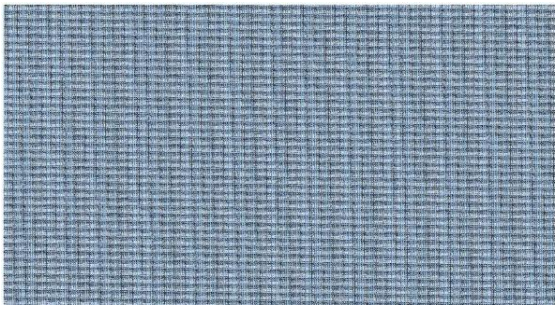

Fig 7: Ciphered image of image 1

Fig 8: Ciphered image of image 2

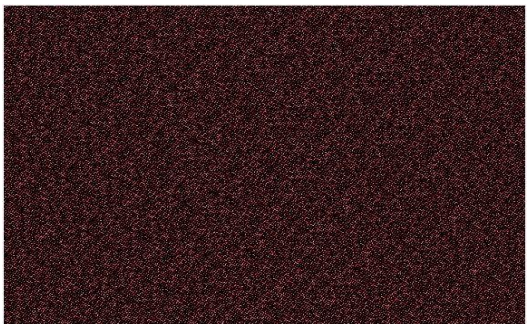

Fig 9: Ciphered image of image 3

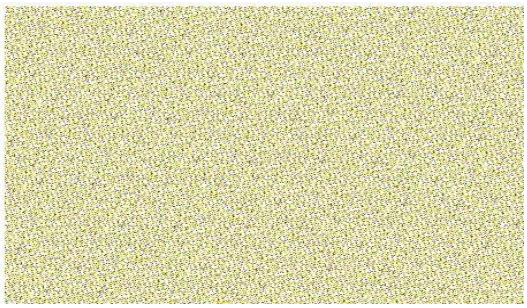

Fig 10: Ciphered image of image 4

6.1 Image Entropy

Entropy measures the uncertainty association with random variable in a system. It is also known as information entropy (He).In a secure cryptographic system, the information entropy of the ciphered image should not provide any information about the plain image. The information entropy was calculated for each iteration step of the algorithm provided in this paper. The results are in table1 below. The entropy was calculated for the first 10000 pixel values of the ciphered images. The results were obtained using ten iteration steps and a graph was plotted using the values as shown in figure 11. The (He) equation used is as follows:

$$He = -\sum_{k=0}^{G-1} P(k).\log_2(P(k)) \quad (1)$$

Where:

He= Entropy of image

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

P (k) = Probability of the occurrence of symbol k

Table 1. Entropy of ciphered images

No of Iterations	Entropy			
	Image 1	Image 2	Image 3	Image 4
1	4.8961	4.7575	0.2216	0.5747
2	7.2043	6.3574	3.2994	3.7812
3	7.2010	6.7154	3.4170	3.8280
4	7.3748	6.7231	3.4132	3.7836
5	7.3502	6.8019	3.4063	3.8127
6	7.3689	6.7786	3.4071	3.8234
7	7.3749	6.7708	3.3839	3.8128
8	7.3704	6.7645	3.4293	3.8348
9	7.3793	6.7759	3.4009	3.8153
10	7.3695	6.7714	3.3925	3.8121

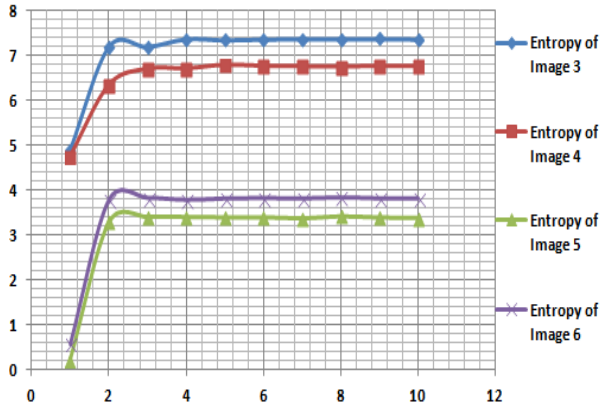

Fig 11: A graph of entropy against number of iterations in table 1

6.2 Arithmetic Mean of Pixel Values

The arithmetic mean or simply the mean or average is the sum of a collection of numbers divided by the number of numbers within the collection. The first 10000 sample pixel values for the encrypted images were extracted from the ciphered image during each turn of encryption using the provided algorithm. The mean of the first 10000 pixel values of the ciphered images was calculated. The results are in table 2 below. The results were obtained using ten iteration steps and a graph was plotted using the values as shown in figure 12. The equation used is as follows:

$$\bar{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \qquad (2)$$

Where:

$\bar{x}$ = Mean

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

Xi = $x_1, \ldots, x_n$ value of an input image (0-255).

Table 2. Entropy of ciphered images

No of Iterations	Mean			
	Image 1	Image 2	Image 3	Image 4
1	177.5632	19.7944	1.2743	251.1219
2	117.5106	49.1109	26.9807	207.6321
3	154.5042	61.2960	29.2535	206.0652
4	146.6116	58.8225	28.8600	207.4197
5	147.6389	60.1695	28.7923	206.5855
6	149.6274	60.0395	28.6780	206.3899
7	149.3406	59.4000	28.4036	206.4776
8	148.9893	59.4756	28.5850	206.2040
9	149.1811	59.4140	28.5509	206.3323
10	148.9654	59.6626	28.4262	206.1601

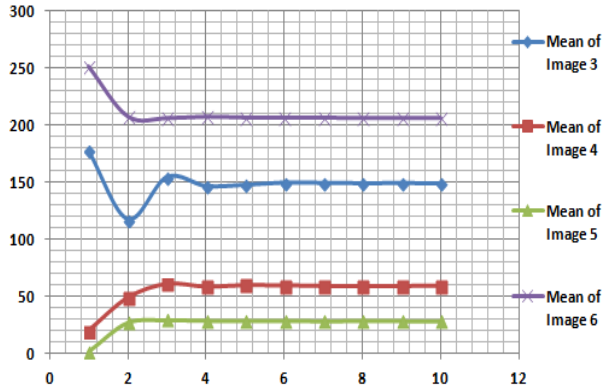

Fig 12: A graph of arithmetic against number of iterations in table 1

Figure 13 and figure 15 represent the RGB graph of the plain images of Figure 3 and figure 4 respectively. And the RGB graphs of the final ciphered image of figure 7 and figure 8 are shown as figure 14 and 16 below. The graphs were plotted using their first 10000 pixel values of the plain and ciphered images.

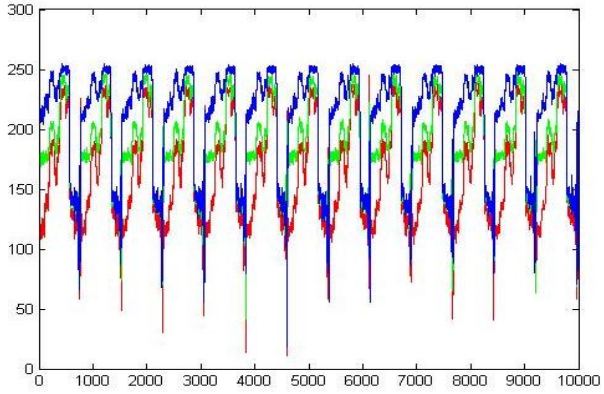

Fig 13: An RBG graph of Figure 3

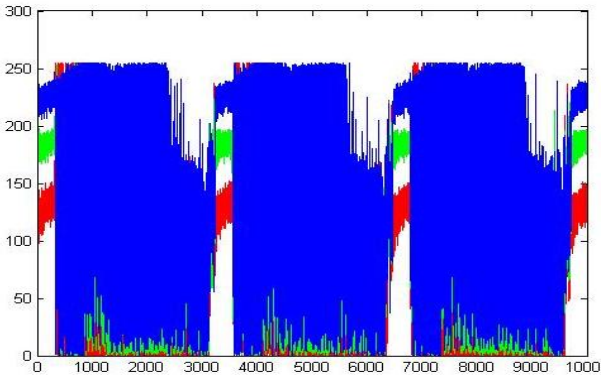

Fig 14: An RBG graph of Figure 7

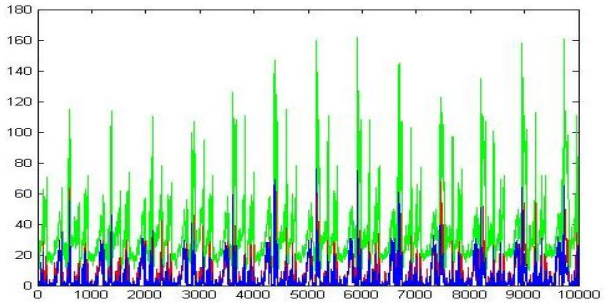

Fig 15: An RBG graph of Figure 4

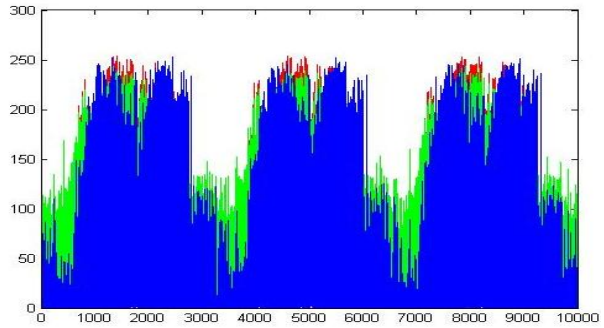

Fig 11: An RBG graph of Figure 8

The overall entropy and mean for the plain images 1, 2, 3, 4 and the ciphered image 1, 2, 3, 4 for table 1 and 2 were found to be 147.9979, 60.6728, 28.6324, 206.4466 and 7.4037, 6.8267 3.4205, 3.8367 respectively.

7. CONCLUSION

From the results, the entropy values for each step in the algorithm proof to be very effective. The values remain approximately close and the ciphered image visually unrecognizable as the iteration of the algorithm increases. This makes the algorithm very efficient. The total entropy of the plain images remained constant for the mxn ciphered images irrespective of the number of iteration performed since there has been no pixel expansion. That is the average total pixel before encryption is the as the average total pixel after encryption.

Our future research work will be focused on the employment of public key cryptography in the encryption of images.

8. 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..

9. REFERENCES

[1] Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966. ISBN 0-88385-622-0

[2] Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT 2002.

[3] Kester, Quist-Aphetsi, and Koudjo M. Koumadi. "Cryptographie technique for image encryption based on the RGB pixel displacement." Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on. IEEE, 2012.

[4] Benhocine, A., Laouamer, L., Nana, L., & Pascu, A. C. (2013). New Images Watermarking Scheme Based on Singular Value Decomposition. Journal of Information Hiding and Multimedia Signal Processing, 4(1), 9-18.

[5] Dang, Philip P., and Paul M. Chau. "Image encryption for secure internet multimedia applications." Consumer Electronics, IEEE Transactions on 46, no. 3 (2000): 395-403

[6] Guo, Jiun-In. "A new chaotic key-based design for image encryption and decryption." In Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 4, pp. 49-52. IEEE, 2000.

[7] 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.

[8] Maksuanpan, S.; San-Um, W., "A new simple digital image cryptography technique based on multi-scroll chaotic Delay Differential Equation," Knowledge and Smart Technology (KST), 2013 5th International Conference on , vol., no., pp.134,138, Jan. 31 2013-Feb. 1 2013 doi: 10.1109/KST.2013.6512802

[9] Wu, Xiaoyu; Wong, Duncan S.; Li, Qing, "Extended Visual Cryptography Scheme for color images with no pixel expansion," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on , vol., no., pp.1,4, 26-28 July 2010

[10] Askari, N.; Heys, H.M.; Moloney, C.R., "An extended visual cryptography scheme without pixel expansion for halftone images," Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on , vol., no., pp.1,6, 5-8 May 2013 doi: 10.1109/CCECE.2013.6567726

[11] Monoth, T.; Babu, A.P., "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns," Cyberworlds (CW), 2010 International Conference on , vol., no., pp.171,178, 20-22 Oct. 2010 doi:10.1109/CW.2010.