ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, January 2013

A cryptographic Image Encryption technique based on the RGB PIXEL shuffling

Quist-Aphetsi Kester, MIEEE

***Abstract*— Confidentiality is one of the ultimate goals in information security. Through encryption one can prevent a third party from understanding raw data during signal transmission. The encryption methods for enhancing the security of digital contents has gained high significance in the current era of breach of security and misuse of the confidential information intercepted and misused by the unauthorized parties. Rigorous use of advanced mathematical algorithms has played a major role in the success of modern day cryptography.**

This paper sets out to contribute to the general body of knowledge in the area of cryptography application and by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The algorithm was implemented using MATLAB.

***Index Terms*— Cryptography, Encryption, pixel, shuffling, algorithm**

I. INTRODUCTION

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 result of the process is encrypted information. 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-Hemal etc[2]

Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. Symmetric-key algorithms [3] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys.

The encryption and decryption process of this paper is based on symmetrical algorithm encryption process. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent.

Enormous number of transfer of data and information takes place through internet, which is considered to be most efficient though it's definitely a public access medium.

***Quist-Aphetsi Kester MIEEE**, Faculty of Informatics, Ghana Technology University College, Accra, Ghana, +233 209822141*

The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc.

One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear [4].

The chaotic confusion and pixel diffusion [5] methods was proposed by Friedrich perform the permutations using a chaotic 2-D [6] combined with alterations of Grey-Level values of each pixel in a sequential manner. Repetitive rounds of permutations and changes were used to achieve higher security. It was experimentally verified that the amount of time overhead in performing complex calculations and the complex diffusion process had led to large time complexity of the system.

When Visual Cryptography is used for secure communications; the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information. [7]

This paper proposes an image based encryption technique by developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel.

The paper has the following structure: section II consist of related works, section III gives information on the methodology employed for the encryption and the decryption process, section IV presents the mathematical algorithms employed to come out with a cipher for the encryption process, section V gives explains the algorithm mathematically by showing the step by step manipulation and shuffling of the image pixels, section VI provided the architectural summary of the encryption and decryption process using flow charts, section VII consist of the simulated results and their mathematical as well as graphical analysis and section VIII concluded the paper.

II. RELATED WORKS

A new cryptographic scheme proposed for securing color image based on visual cryptography scheme was done by Krishnan, G.S. and Loganathan, D. A binary image was used as the key input to encrypt and decrypt a color image. The secret color image which needs to be communicated was decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images were then converted into binary image, and finally the obtained binary images were encrypted using binary key image, called share-1, to obtain the binary cipher images. During their encryption process, exclusive OR operation was used between binary key image and three half-tones of secret color image separately. These binary images were combined to obtain share-2. In the decryption process, the shares were decrypted, and then the recovered binary images were inversed half toned and combined to get secret color image. [8]

With extended Visual Cryptography, which is a method of cryptography that reveals the target image by stacking meaningful images. Christy and Seenivasagam proposed a method that uses Back Propagation Network (BPN) for extended visual cryptography. BPN was used to produce the two shares. The size of the image produced was the same as that of the original image. [9]

A k-out-of-n Extended Visual Cryptography Scheme (EVCS) is a secret sharing scheme which hides a secret image into n shares, which are also some images. 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 are either for black-and-white images or having pixel expansion. Wu, Xiaoyu, Wong, Duncan S. and Li, Qin proposed the first k-out-of-n EVCS for color images with no pixel expansion. The 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. [10]

Kester, QA proposed a cryptographic algorithm based on matrix and a shared secrete key.[11]. Which was further applied encryption and decryption of the images based on the RGB pixel [12].

Shujiang Xu,Yinglong Wang , Yucui Guo and Cong Wanga proposed a novel image encryption scheme based on a nonlinear chaotic map (NCM) and only by means of XOR operation. There were two rounds in the proposed image encryption scheme. In each round of the scheme, the pixel gray values were modified from the first pixel to the last pixel firstly, and then the modified image was encrypted from the last pixel to the first pixel in the inverse order. In order to accelerate the encryption speed, every time NCM was iterated, n (n>3) bytes random numbers were used to mask the plain-image. And to enhance the security, a small perturbation was given to the parameters of the NCM based on the last obtained n bytes modified elements before next iteration. [13]

Ruisong Ye and Wei Zhou proposed a chaos-based image encryption scheme where one 3D skew tent map with three control parameters were utilized to generate chaotic orbits applied to scramble the pixel positions while one coupled map lattice was employed to yield random gray value sequences to change the gray values so as to enhance the security. Experimental results have been carried out with detailed analysis to demonstrate that the proposed image encryption scheme possesses large key space to resist brute-force attack and possesses good statistical properties to frustrate statistical analysis attacks. And at the end, the proposed scheme utilizes the 3D skew tent map to shuffle the plain-image efficiently in the pixel Positions permutation process and it employed the coupled map lattice system to change the gray values of the whole image pixels greatly.[14]

With the exceptionally good properties in chaotic systems, such as sensitivity to initial conditions and control parameters, pseudo-randomness and ergodicity, chaos-based image encryption algorithms have been widely studied and developed in recent years. Standard map is chaotic and it can be employed to shuffle the positions of image pixels to get a totally visual difference from the original images.

Ruisong Ye,Huiqing Huang proposed two novel schemes to shuffle digital images. Different from the conventional schemes based on Standard map, they disordered the pixel positions according to the orbits of the Standard map. The proposed shuffling schemes didn't need to discretize the Standard map and own more cipher leys compared with the conventional shuffling scheme based on the discretized Standard map. The shuffling schemes were applied to encrypt image and disarray the host image in watermarking scheme to enhance the robustness against attacks. [15]

Amnesh Goel and Nidhi proposed contrastive methods to encrypt images by introducing a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. [16]

Image Encryption Based on Explosive Inter Pixel Displacement of the RGB Attribute of a Pixel: In this method focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method. In the similar manner, G and B values of pixel [17].

With the proposed method in this paper, the shuffling of the image will be done by solely displacing the RGB pixels and also interchanging the RGB pixel values. At the end the total image size before encryption will be the same as the total image size after encryption.

III. METHODOLOGY

The images used will have their RGB colors extracted from then and manipulated to obtain the ciphered image. The ciphering of the image for this research will be done by using the RBG pixel values of the images.

In this method, there are no changes of the bit values and there is no pixel expansion at the end of the encryption and the decryption process. Instead the numerical values are

transposed, reshaped and concatenated with the RGB values shifted away from its respective positions and the RGB values interchanged in order to obtain the cipher image. This implies that, the total change in the sum of all values in the image is zero. Therefore there is no change in the total size of the image during encryption and decryption process. The characteristic sizes of image will remain unchanged while the encryption process is being performed.

The image is looked at as a decomposed version in which the three principle component which forms the image is chosen to act upon by the algorithm. The R-G-B components can be considered as the triplet that forms the characteristics of a pixel. The pixel is the smallest element of an image which can be isolated and still contains the characteristic found in the image.

The RGB values are shifted out of its native pixel and interchanged within the image boundaries by the algorithmic process. The Shift displacement of the R G and B Values known termed as the component displacement factor array which is different for R, G and B.

With the proposed method in this paper, the shuffling of the image will be ultimately done by solely displacing the RGB pixels and also interchanging the RGB pixel values.

IV. THE ALGORITHM

1. .Start
2. Import data from image and create an image graphics object by interpreting each element in a matrix.
3. Extract the red component as ‘r’
4. Extract the green component as ‘g’
5. Extract the blue component as ‘b’
6. Get the size of r as [c, p]
7. Let r =Transpose of r
8. Let g =Transpose of g
9. Let b =Transpose of b
10. Reshape r into (r, c, p)
11. Reshape g into (g, c, and p)
12. Reshape b into (b, c, and p)
13. Concatenate the arrays r, g, b into the same dimension of ‘r’ or ‘g’ or ‘b’ of the original image.
14. Finally the data will be converted into an image format to get the encrypted image.

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

V. THE MATHEMATICAL EXPLANATION

Step1. Start

Step2. Import data from image and create an image graphics object by interpreting each element in a matrix.

Let Q= an image=Q(R, G, B)

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

$$\begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ r_{n1} & g_{n2} & b_{n3} \end{pmatrix}$$

(R, G, B) = m x n

Where R, G, B ∈ R

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

Where R= r_i1 = 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= Q(m,n,1)

Where G= g_i2 = 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= Q(m,n,1)

And B= b_i3 = 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= Q (m, n, 1)

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

Extract the red component as ‘r’

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

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

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

Step4. Extract the green component as ‘g’

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

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

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

Step5. Extract the blue component as 'b'

Let size of B be m x n [row, column] = size (B) = B (m x n)

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

$$\begin{pmatrix} B \\ b_{i3} \\ \vdots \\ b_{n3} \end{pmatrix}$$

Step6. Get the size of r as [c , p]

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

Step7. Let r =Transpose of r

r =

$$\begin{pmatrix} R & & & & \\ r_{i1} & \cdots & \cdots & \cdots & r_{n1} \end{pmatrix}$$

Step8. Let g =Transpose of g

g =

$$\begin{pmatrix} G & & & & \\ g_{i3} & \cdots & \cdots & \cdots & g_{n3} \end{pmatrix}$$

Step9. Let b =Transpose of b

b=

$$\begin{pmatrix} B & & & & \\ b_{i2} & \cdots & \cdots & \cdots & b_{n2} \end{pmatrix}$$

Step10. Reshape r into (r, c, p)

r= reshape (r, c, p) =

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

Step11. Reshape g into (g ,c ,p)

g= reshape (g, c, p) =

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

Step12. Reshape b into (b ,c ,p)

b= reshape (b, c, p) =

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

Step13. Concatenation of the arrays r, g, b into the same dimension of 'r' or 'g' or 'b' of the original image

=

$$\begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ r_{n1} & g_{n2} & b_{n3} \end{pmatrix}$$

Step14. Let y 14. Finally the data will be converted into an image format to get the encrypted image.

The inverse of the algorithm will decrypt the encrypted image

VI. ARCHITECTURAL SUMMARY OF THE ENCRYPTION AND DECRYPTION PROCESS USING FLOW CHART DIAGRAM

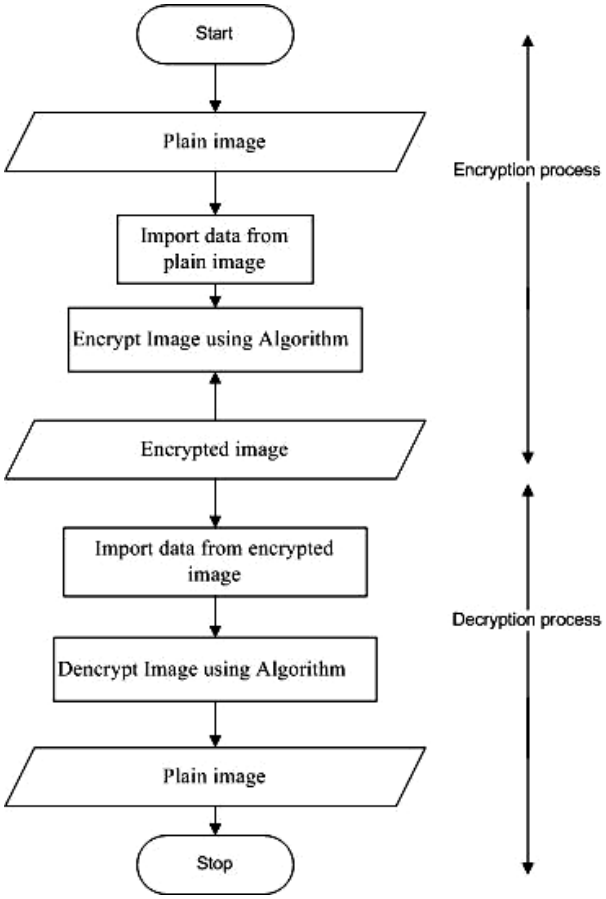

Fig 1 .Flow chart diagram for the encryption and decryption process

Figure 1 showed the flow chart diagram for the encryption and decryption process.

VII. SIMULATED RESULTS

The simulation of the above algorithm was performed on the MATLAB Version 7.0.0.1 to verify the effectiveness of the proposed algorithm. The plain image size used was m x n. The MATLAB code for the algorithm was written and tested the output is shown below.

Fig 2. Plain image of Chrysanthemum from Microsoft windows7 sample pictures

Fig 3. Ciphered image of Chrysanthemum from figure2

Fig 4. Plain image of Penguins from Microsoft windows7 sample pictures

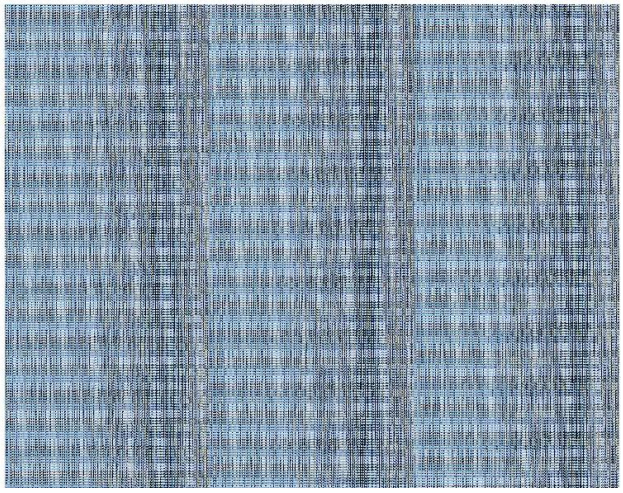

Fig 5. Ciphered image of Penguins from figure 4

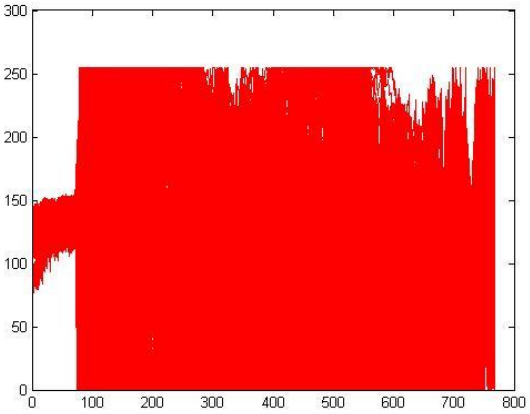

Fig 6. Figure 6 An R graph of plain image of Figure 4

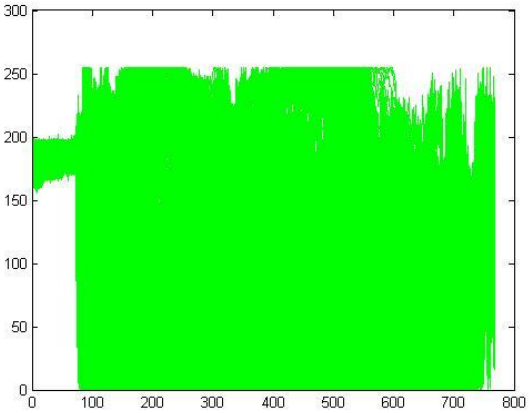

Fig 7. Figure 6 A G graph of plain image of Figure 4

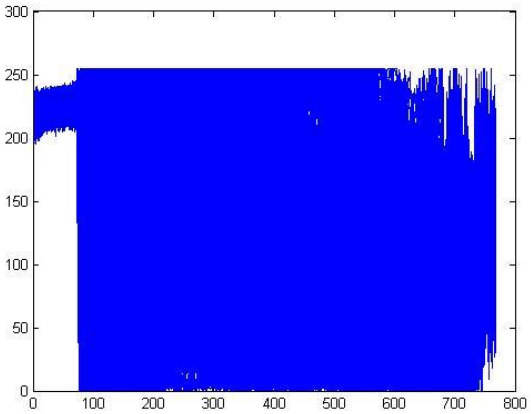

Fig 8. Figure 6 A B graph of plain image of Figure 4

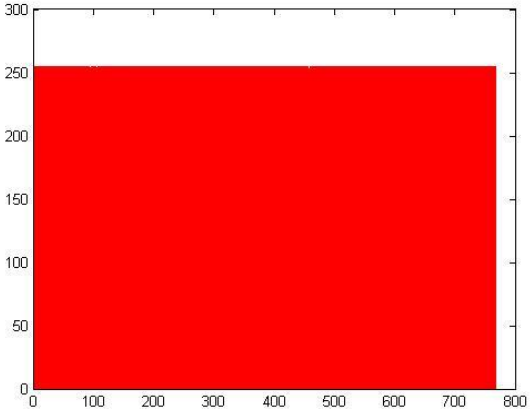

Fig 9. An R graph of cipher image of Figure 5

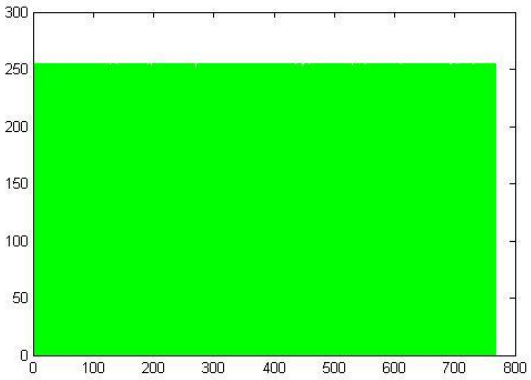

Fig 10. A G graph of cipher image of Figure 5

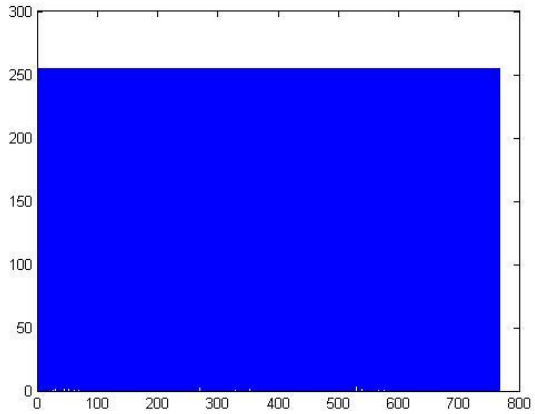

Fig 11. A B graph of cipher image of Figure 5

VIII. DISCUSSION AND CONCLUSION

The pixel displacement and reshuffling of the image in steps between the processes has proven to be really effective in terms of the security analysis. The extra transposition of RGB values in the image file after R G B component reshape has proven the increase of security of the image against all possible attacks available currently.

Our future research on this is focused on the employment of public key cryptography in the encryption of images.

REFERENCES

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

[2] Kester, Quist-Aphetsi. "A cryptosystem based on Vigenère cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1, no. 10 (2012): pp-108.

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

[4] Visual cryptography retrieved from: http://en.wikipedia.org/wiki/Visual_cryptography

[5] M. Salleh, S Ibrahim and I.F. Isnin, Image encryption algorithm based on chaotic mapping.JurnalTeknologi, 39(D) Dis. 2003: 1–12 UniversitiTeknologi Malaysia.

[6] R.Kadir, R.Shahri and M.A.Maarof, A modified image encryption scheme based on 2D chaotic map. 978-1-4244-6235-3/10/2010 IEEE.

[7] Dirk Rijmenants Visual Cryptography retrieved from: http://users.telenet.be/d.rijmenants/en/visualcrypto.htm

[8] Krishnan, G.S.; Loganathan, D.; , "Color image cryptography scheme based on visual cryptography," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.404-407, 21-22 July 2011

[9] Christy, J.I.; Seenivasagam, V.; , "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images," Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1101-1108, 21-22 March 2012

[10] 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

[11] Kester, Quist-Aphetsi; , "A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012

[12] Kester, Quist-Aphetsi; Koumadi, Koudjo M; , "Cryptographie technique for image encryption based on the RGB pixel displacement," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.74-77, 25-27 Oct. 2012

[13] Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010.

[14] Ruisong Ye,Wei Zhou,"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", IJCNIS, vol.4, no.1, pp.38-44, 2012.

[15] Ruisong Ye,Huiqing Huang, "Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking", IJIGSP, vol.2, no.1, pp.19-29, 2010.

[16] Amnesh Goel,Nidhi Chandra,"A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", IJIGSP, vol.4, no.2, pp.16-22, 2012.

[17] Reji Mathews, Amnesh Goel, PrachurSaxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

Quist-Aphetsi Kester MIEEE: is a global award winner 2010 (First place Winner with Gold), in Canada Toronto, of the NSBE's Consulting Design Olympiad Awards and has been recognized as a Global Consulting Design Engineer. Currently the national chair for Policy and Research Internet Society (ISOC) Ghana Chapter, a world renowned body that provides international leadership in Internet related standards, education, and policy. He is a law student at the University of London UK. He is a PhD student in Computer Science. The PhD program is in collaboration between the AWBC/ Canada and the Department of Computer Science and Information Technology (DCSIT), University of Cape Coast. He had a Master of Software Engineering degree from the OUM, Malaysia and BSC in Physics from the University of Cape Coast-UCC Ghana.

He has worked in various capacities as a peer reviewer for IEEE ICAST Conference, IET-Software Journal, lecturer, Head of Digital Forensic Laboratory Department at the Ghana Technology University and Head of Computer science department. He is currently a lecturer at the Ghana Technology University College.