ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 7, July 2013

Enhancement of the Security of a Digital Image using the Moduli Set $\{2^n - 1, 2^n, 2^n + 1\}$

S. Alhassan, K.A. Gbolagade

***Abstract*—** Digital images have found usage in many applications. These images may contain confidential information and need to be protected when stored on memory or transmitted over networks. Many techniques have been proposed to deal with this security issues. In this paper, we propose a new security enhancement scheme for digital images. The scheme employs two methods: Residue Number System (RNS) to Decimal (R/D) encoding and decoding using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ and a modified Arnold transform algorithm. The encryption process uses RNS to Decimal (D/R) converter (encoder) to decompose a plain image into three residual images. The residual images are fused together and encrypted using the modified Arnold transform. In the decryption process, the modified Arnold transform is used to decrypt the cipher image which is then decomposed into three residual images. An R/D converter (decoder) is then used to recover the plain image. The proposed scheme is simulated on digital images of different sizes using MATLAB. The obtained results show that the scheme can effectively encrypt and decrypt images without lost of any inherent information. The scheme also offers firm resistance to statistical attacks such as histogram, brute-force, correlation coefficient and key sensitivity. It can be applied to any shape of image and allow unlimited number of iterations to be performed as opposed to best known state of the art.

***Index Terms*—**D/R encoder, R/D decoder, residual image, Residue Number System, Arnold transform.

I. INTRODUCTION

The security of information and digital images has become a major concern for the past few decades due to the rapid advancement in internet and networking technologies. Images have found usage in diverse areas such as medical, military, science, engineering, art, entertainment, advertising, and education. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Over the years, various hidden and secret communication techniques aimed at addressing this need, have been proposed [1-15].

A lot of image scrambling techniques have been developed to improve the security level of hidden information [1-15]. Image scrambling techniques scramble the pixel location of digital images in such a manner that they become chaotic and indistinguishable [11]. These techniques generally use several keys for encryption and decryption and without the correct keys and an appropriate method and attackers cannot access the secret information even if they are able to sniff the medium. Hence, the message remains highly secured against unauthorised access [11].

The traditional Arnold cat map has been extensively refined to strengthen its security [3], [11, [13]. However, these techniques mainly apply only to square images and their strength lie on periodicity. The techniques also merely scramble the pixel position of the image.

Mohammad [12] proposed a block-based transformation algorithm based on the combination of image transformation and an encryption and decryption algorithm called Blowfish. Katherine [5] used both the Arnold Cat Map to shuffle pixel values and Chen's chaotic map to change the grayscale values of the pixels. Musheer et al. [13] proposed a new image encryption algorithm based on three different chaotic maps. In [13], the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map. Chattopadhyay et al. [3] proposed a novel algorithm for encoding digital images by using a circle map with 3 parameters. The algorithm [3] showed an increase in security against cipher-text-only, chosen-plaintext and chosen-cipher-text attacks. Minati [11] proposed an image scrambling map based on Fibonacci and Lucas series which can be used in various spatial domain image processing techniques of data hiding and secret communications.

In this paper we focus on the security mechanism of digital image namely encryption and decryption using a modified Arnold transform and Residue Number System (RNS). We propose in here an image encryption and decryption algorithm using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$, and demonstrate that the algorithms successfully hide and recover the plain image without lost of any inherent information.

The rest of the paper is structured as follows: a brief discussion of Arnold transform and RNS is presented in Section 2. A detailed discussion of the proposed scheme is covered in Section 3. Section 4 presents experimental results and discussion on the scheme. Finally, Sections 5 and 6 look at the concluding remarks and future works, respectively.

II. BACKGROUND INFORMATION

A. Arnold Transform

The Arnold transform is defined as the transformation [11] $\Gamma: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ such that;

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \qquad (1)$$

where, $x, y \in \{0, 1, 2\ \ldots\ N-1\}$ and N is the size of the digital image. (x', y') is the new position of the original pixel position (x, y) of the N x N plain-image.

A new image is produced when all the points are manipulated by Equation (1).

B. Residue Number System (RNS)

RNS comprises a set of moduli which are independent of each other. An integer is represented by the residue of each of the modulus and arithmetic operations are based on residues individually. The advantage of using the RNS over the conversional system includes "carry-free" operation, fault tolerance, parallelism and modularity. These inherent features make RNS to be widely used in Digital Signal Processing (DSP) applications such as digital filtering, convolution, fast Fourier transform and image processing [18].

Let $\{m_1, m_2, m_3, \ldots, m_n\}$ be a set of positive integers all greater than 1. m_i is called a modulus, and the n-tuple set $\{m_1, m_2, m_3, \ldots, m_n\}$ is called a moduli set. Consider an integer number Y. For each of the modulus in $\{m_1, m_2, m_3, \ldots, m_n\}$, we have $y_i = Y\ mod\ m_i$, (which will be denoted as $|Y|_{m_i}$). Thus the number Y in this system is represented as $Y = (y_1, y_2, y_3, \ldots, y_n)$, $0 \leq y_i < m_i$.

Given the moduli set $\{7, 8, 9\}$, the number 150 can be represented in RNS as

$y_1 = |Y|_{m_1} = |150|_7 = 3$,
$y_2 = |Y|_{m_2} = |150|_8 = 6$ and
$y_3 = |Y|_{m_3} = |150|_9 = 6$. Thus, the RNS representation of 150 is thus: $(3, 6, 6)_{RNS(7,8,9)}$.

To avoid redundancy, the moduli set must be pairwise relatively prime. Thus, $\gcd(m_i, m_j) = 1$ for $i \neq j$, where $\gcd$ means the greatest common divisor of m_i and m_j.

Let $M = \prod_{i=1}^{n} m_i$, then the RNS representation is unique for any integer $Y \in [0, M-1]$. M is called the dynamic range [18], [19].

A Decimal to Residue (D/R) converter (encoder) is needed in order to convert a decimal number to RNS representation.

C. RNS to Weighted Conversion

A Residue to Decimal (R/D) converter (decoder) is required in other to convert from a RNS to decimal. The two method used to convert RNS to weighted system are the Chinese Remainder Theorem (CRT) and the Mixed Radix Conversion (MRC). The CRT is employed in this research. The CRT is defined as follows [19].

Given a moduli set $\{m_1, m_2, m_3, \ldots, m_n\}$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and dynamic range $M = \prod_{i=1}^{n} m_i$, then by the CRT an integer Y whose RNS representation is $(y_1, y_2, y_3, \ldots, y_n)$ can be converted from its residue form as

$$Y = \left| \sum_{i=1}^{n} M_i \left| M_i^{-1} y_i \right|_{m_i} \right|_M, \qquad (2)$$

where $M_i = \frac{M}{m_i}$ and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i.

A schematic diagram of the CRT is showed in Fig. 1.

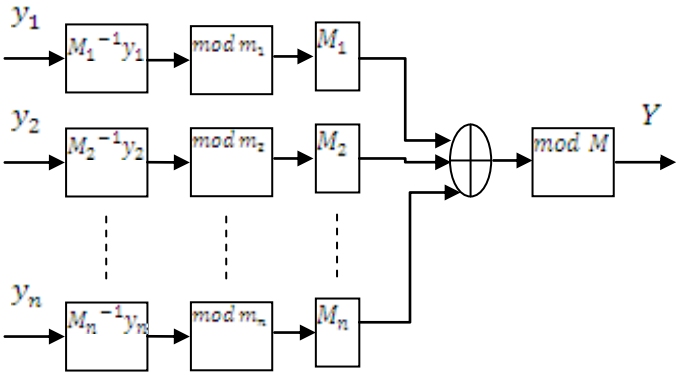

Fig. 1. Schematic diagram of the CRT

For example, given the moduli set $\{7, 8, 9\}$, $= 10 = (3, 2, 1)$, $M = 7 \times 8 \times 9 = 504$,

$$M_1 = \frac{504}{7} = 72, \quad M_2 = \frac{504}{8} = 63,$$
$$M_3 = \frac{504}{9} = 56$$

$$M_1^{-1} = 72^{-1} = 4,\ M_2^{-1} = 63^{-1} = 7,$$
$$M_3^{-1} = 56^{-1} = 5$$

Therefore by the CRT

$$Y = |(72 \times |4 \times 3|_7) + (72 \times |7 \times 2|_8) + (56 \times |5 \times 1|_9)|_{504}$$

$$Y = |(72 \times 5) + (72 \times 6) + (56 \times 5)|_{504}$$
$$Y = |360 + 378 + 280|_{504}$$
$$Y = |1018|_{504}$$

Hence; $Y = 10$

III. PROPOSED SCHEME

Encryption and decryption algorithms are formulated by integrating a modified Arnold's transform algorithm, and the Chinese Remainder Theorem (CRT). The algorithms are tested on both grayscale and true color images of varying sizes through simulating with MATLAB.

A. Encryption process

The encryption algorithm takes a plain image and transforms it into a cipher image. The inputs to the algorithm are $n \geq 3$ (for moduli set), $k \in \mathbb{Z}$ (a constant), $p = 1,2$ ...(number iterations) and T (an $n\ x\ m$ plain image). The output of this algorithm is an $(n * 3)\ x\ m$ augmented cipher image $\overline{T}$.

1) Pixel Encoding

The encoding process transforms an $n\ x\ m$ plain image T into an augmented $(n * 3)\ x\ m$ encoded image T_r by using Equation (3).

$$T_r = \left[|T|_{m_1}; |T|_{m_2}; |T|_{m_3}\right] \qquad (3)$$

2) Pixel Scrambling

The augmented image T_r is then randomised by using the modified Arnold transform presented in Equation (4) into cipher image $\overline{T}$;

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left(\begin{pmatrix} m_1 & m_2 \\ k & m_3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + (p) \right) (mod\ N) \qquad (4)$$

where $x, y \in \{1, 2, 3, \ldots N\}$, m_1, m_2, m_3 correspond to the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$, $n \geq 3, k \in \mathbb{Z}$, $p = 1,2, \ldots$ and N is $2\ x\ 1$ vector $\begin{Bmatrix} n \\ m \end{Bmatrix}$ refers to the size of the image.

3) The Encryption Algorithm

The algorithm for the encryption process is as follows:

1) Input n, k, p and plain image T
2) Obtain the values of m_1, m_2, m_3 using $\{2^n - 1, 2^n, 2^n + 1\}$
3) Using Equation (3), transform T into the augmented image T_r.
4) For $i = 1\ to\ p$
   Scramble T_r into the cipher image $\overline{T}$ using Equation (4)
4) Save $\overline{T}$

A flow diagram of the encryption process is shown in Fig. 2.

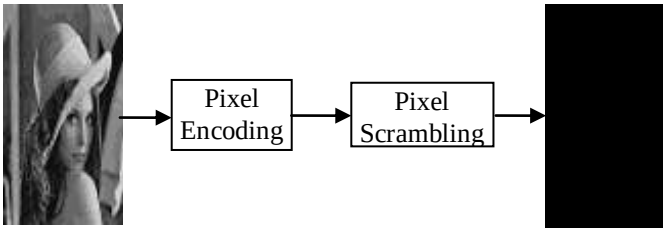

Fig. 2. Flow diagram of the encryption process.

B. Decryption Process

The decryption process is a reverse of the encryption process. It takes an $(n * 3)\ x\ m$ cipher image and transforms it into an $n\ x\ m$ plain image. This process has three stages; anti-Arnold's transform, decomposition process, and decoding using CRT.

1) Pixel Scrambling

The pixels positions of the cipher image $\overline{T}$ have to be reorganised. This is achieved by applying Equation (4) in reverse order. In doing this, the pixel values are returned to their respective original positions to form the cipher image T_r.

2) Cipher Image Decomposition

The $(n * 3)\ x\ m$ cipher image T_r resulting from scrambling process is decomposed into three $n\ x\ m$ cipher images as follows in Equations (5),(6), and (7);

Let $\overline{T}_1$, $\overline{T}_2$ and $\overline{T}_3$ be $n\ x\ m$ decomposed cipher images and $\bar{n}\ x\ \bar{m}$ the dimension of T_r then,

$$\overline{T}_1 = T_r\left[1, \frac{\bar{n}}{3}\right] \qquad (5)$$

$$\overline{T}_2 = T_r\left[\left(\frac{\bar{n}}{3} + 1\right), \left(\frac{\bar{n}}{3} x\ 2\right)\right] \qquad (6)$$

$$\overline{T}_3 = T_r\left[\left(\frac{\bar{n}}{3} x\ 2\right) + 1, \bar{n}\right] \qquad (7)$$

In Equations (5), (6) and (7) respectively isolates three cipher images corresponding to each of the three modulus operations in Equation (3).

3) Pixel Decoding Using CRT

The three residual images obtained in the decomposition process are then used to recover the pixels of the plain image. In this regard, we implement Equation (2) using the pixels of the decomposed images $\overline{T}_1$, $\overline{T}_2$ and $\overline{T}_3$. Thus;

Given that $\{r_1, r_2, r_3\}$ are the residues of each original pixel X in T with respect to $\{m_1, m_2, m_3\}$ then,

$$X = (\overline{T}_1(i,j), \overline{T}_2(i,j), \overline{T}_3(i,j)) \qquad (8)$$

where $i = 1,2, \ldots n, j = 1,2, \ldots m$ and

$r_1 = \overline{T}_1(i,j), r_2 = \overline{T}_2(i,j)$ and $r_3 = \overline{T}_3(i,j)$

4) The Decryption Algorithm

The decryption algorithm is formulated as follows:

1) Input n, k, p and cipher image $\overline{T}$
2) Obtain $\{m_1, m_2, m_3\}$ using $\{2^n - 1, 2^n, 2^n + 1\}$
3) For $i = p$ down to 1
   Scramble $\overline{T}$ into T_r using Equation (3)
4) Decompose T_r into $\overline{T}_1$, $\overline{T}_2$ and $\overline{T}_3$ using Equations (5), (6) and (7)
4) Using Equations (2) and (8) recover the plain image T from $\overline{T}_1$, $\overline{T}_2$ and $\overline{T}_3$
6) Save T

The complete decryption process is shown in Fig. 3.

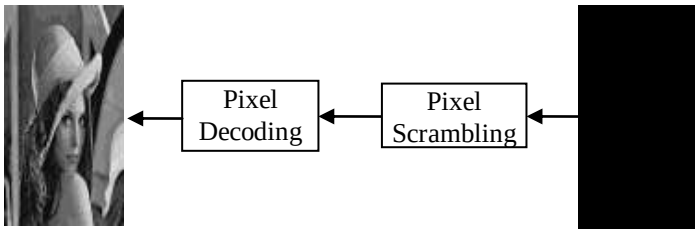

Fig. 3. Flow diagram of the encryption process.

IV. EXPERIMENTAL RESULTS

In this section, a detail analysis of the proposed scheme has been summarized. Simulations were conducted using MALTAB. The analyses include visual testing, encoding analysis and security analysis. Experimental results suggest that the proposed scheme is more efficient than the proposal in Minati, et al [11] in terms of encoding and security.

A. Visual Testing

Three images of varying size, both grayscale and colour were used. Fig. 4 depicts test results for the images (lena (512 x 512), koala (448 x 336) and checkerboard (256 x 256)). The visual test clearly shows the absence of similarities among the pairs of images.

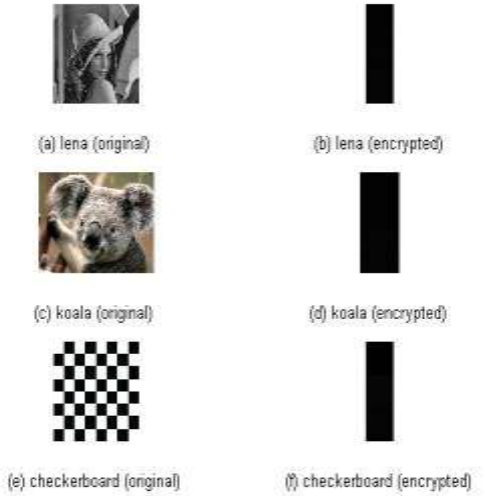

Fig. 4. Original and encrypted images for $n = 3, k = 2, p = 15$.

Visual tests were also performed to check whether the proposed scheme totally recovers plain images. Fig. 5 shows the histograms of both original and decrypted images. It can be seen from the similarities of both histograms that the proposed scheme totally recovers plain images.

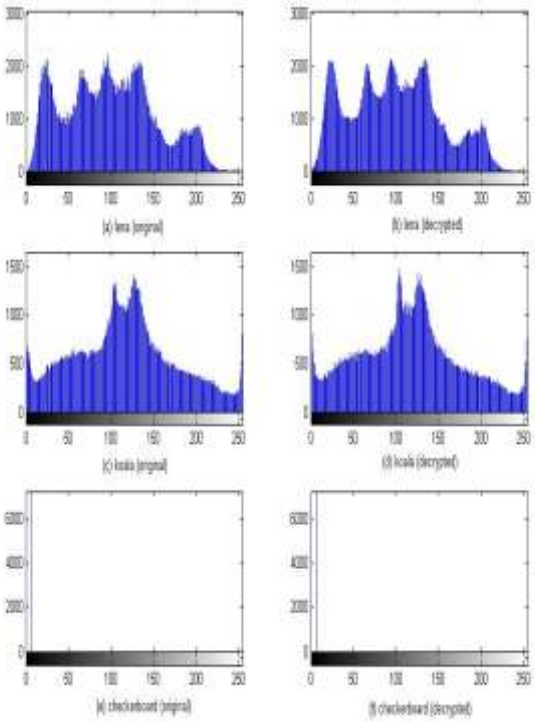

Fig. 5. Histograms of original and decrypted images $n = 3, k = 2, p = 15$. (a) Original "lena" histogram (upper left), (b) Decrypted "lena" histogram (upper right), (c) Original "koala" histogram (middle left), (d) Decrypted "koala" histogram (middle right) , (e) Original "checkerboard" histogram (bottom left), (f) Decrypted "checkerboard" histogram (bottom right).

B. Encoding Analysis

The pixel encoding during the encryption process achieves two results. It reduces the pixel value and the size (in terms of disk space) of the plain image but retains its physical. The reduction in pixel value speeds up computation which is useful during other image processing techniques. On the other hand the reduction in size speeds up data transmission across network since fewer bits are required to represent the pixels. Table I compare the size of both plain and cipher images when save in a JPEG format. It can be deduced from the table that for $n = 3$ the proposed system achieves a reduction in size by up to 90%.

Table I. Disk sizes of plain and cipher images compared

Image Type	**Size(disk space)**		
	Plain image	**Cipher image**	**Compression ratio**
lena.jpg(512x512)grayscale	152 kb	26.7 kb	82.43%
Easy.bmp(640x480) colour	301 kb	31.7 kb	92.45%
pic.png(320x301) colour	163 kb	7.06 kb	95.66%

C. Security Analysis

In this subsection, we analyse the security and strength of our encryption scheme. Areas assessed include histogram analysis, key space, key sensitivity and correlation coefficient analysis

1) Histogram Analysis

The histogram of an image refers to a histogram of the pixel intensity value. It is a graph that shows the number of pixels in an image at each different intensity value found in that image. A cipher image is more secured against statistical attack when its histogram conceals any information about the plain image and also completely defers from the histogram of its plain image. Fig. 6 shows the histograms of a plain image and its cipher image. It is very apparent from the figure that the two histograms are completely different and thus the histogram of the cipher image does not give any clue about the plain image. This implies that the proposed system is secure against histogram attack.

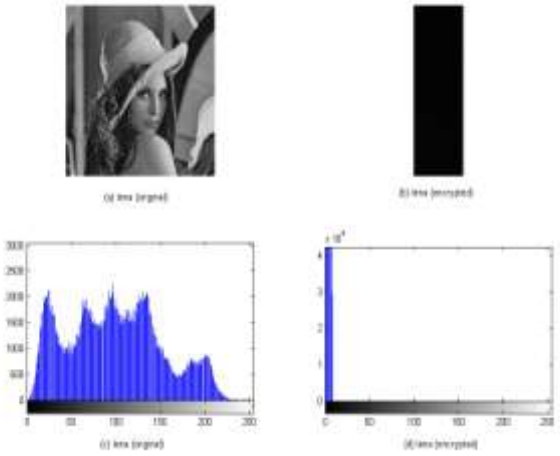

Fig. 6. Histograms of plain and encrypted "lena" images. (a) Original image (upper left), (b) Encrypted image (upper right), (c) Original histogram (bottom left), (d) Encrypted histogram (bottom right).

2) Key Space Analysis

The brute-force attack is computationally infeasible for cryptosystems with sufficiently large key space. The proposed scheme uses a combination of three cipher keys (n, k, p). The scheme achieves an efficient encoding goal when $n = \{3,4,5,6,7\}$. As $k \in \mathbb{Z}$ and $p = 1,2,3, \ldots$ a wide range of combination can be made. However, we adapt a 56 bits key for k, and p as used in Data Encryption Standard (DES). This gives us $2^4 \times 2^{56} \times 2^{56} \cong 8.3077e + 034$ possible combination. Also, suppose an adversary try guessing a key combination with a 1000 MIPS computer, then he/she has $\frac{2^4 \times 2^{56} \times 2^{56}}{1000 \times 10^6 \times 60 \times 60 \times 24 \times 360} > 1000$ years . Clearly this is a long enough time to resist brute-force attack.

3) Key Sensitivity Analysis

A good cryptosystem should be sensitive to the cipher key. A slight change in the key value should lead to a significant change in either plain image or cipher image. In this respect, we present two results to illustrate the key sensitivity of the proposed scheme. The first result shown in Fig. 5 shows that the proposed scheme can successfully decrypt images without any loss of inherent information. On the other hand Fig. 7 shows decrypted images of Fig. 4 (b) with a different value of one of the parameter while maintaining the other two. The unsuccessful decrypted images attest to the fact that the proposed scheme is sensitive to the cipher keys.

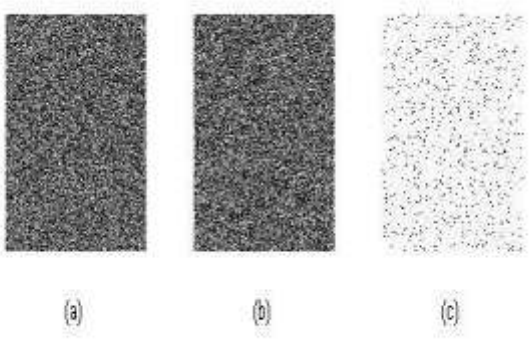

Fig. 7. Key sensitivity analysis (a) Decrypted image with $k = -2$ (b) Decrypted image with $p = 14$ (c) Decrypted image with $n = 4$

4) Correlation Coefficient Analysis

A digital image is meaningful to human vision if there is a high correlation among adjacent pixels. Disturbing this relationship will affect the visual identity of the image. Among the requirements of an effective encryption scheme is creating cipher images that have significantly low correlation coefficient values. For this analysis, we computed the correlation coefficients of randomly selected 1000 pairs of two adjacent pixels (horizontal, vertical and diagonal) of both plain and cipher images.

The correlation coefficient of pairs of adjacent pixels is as follows [21]:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad (9)$$

with $D(x) \neq 0$ and $D(y) \neq 0$

where x and y represent grayscale value of adjacent pixels in the image, and

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,$$
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$cov(x,) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$

Applying Equation (9) on a 512 x 512 'lena.jpg' grayscale image gives the high correlation coefficient values of 0.97184002, 0.98309393, and 0.94877370, respectively for horizontal, vertical and diagonal pairs of adjacent pixels. Table II shows the corresponding correlation coefficient values of cipher images generated for $n = 3,\ k = 2$ and varying values of p. The result shows that the cipher images have weak correlation coefficient values (approximately zero) among pairs of adjacent pixels.

Table II Correlation coefficients of adjacent pixels of a cipher image

iteration	**Adjacent pixels**		
p	Horizontal	Vertical	Diagonal
1	0.02520737	0.06345870	0.03856429
2	0.03821026	0.01262754	0.04166987
3	0.02623524	0.00114685	-0.01844500
10	0.08843156	-0.01475551	0.01968406
15	-0.02460013	-0.02508439	0.01222209

V. CONCLUSION

In this paper, a new image encryption algorithm has been presented. We hold the idea that the security of a cryptosystem would be strengthened if pixel scrambling is fused with encoding. Thus, the proposed scheme has two major parts; pixel value encoding/decoding and pixel scrambling. Experimental results reveal the following;

a) cipher images requires fewer number of bits to represent pixels.
b) the scheme strongly resist to statistical attacks (brute-force, correlation coefficient and histogram.
c) decryption does not depend on periodicity. Thus the number of iterations to conduct is at the discretion of the user.
d) the scheme is also highly sensitive to a small change in any of the cipher keys.

The above mentioned points make our proposed scheme outperform that proposed by Minati, et al [13].

VI. FUTURE WORK

Even though the proposed scheme is efficient in the areas mentioned above, its drawback is the augmented cipher image produced. Thus, cipher images require three times the original memory allocation. A 512 x 512 plain image using 262144 bytes of memory allocation results in a 1536 x 512 (i.e. 512*3 x 512) cipher image using 786432 bytes. Reducing the size of the cipher image without lost any inherent information has been left as a subject of future investigation.

REFERENCES

[1] A. Mitra, Y.V.R. Subba and S.R.M Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering 1:2 2006.
[2] B.A. Weyori, P.N. Amponsah and P.K. Yeboah, "Modeling a Secured Digital Image Encryption Scheme Using a Three Moduli Set", Global Journal of Computer Science and Technology Interdisciplinary, Vol. 12, Issue 10 Version 1.0, 2012
[3] D. Chattopadhyay, M.K. Mandal and D. Nandi, "Symmetric key Chaotic Image Encryption using Circle Map", Indian Journal of Science and Technology, Vol. 4, No. 5, pp. 593-599 May, 2011.
[4] G. Peterson, "Arnold's Cat Map", 2003-04-10], http://online.redwoods.cc.ca.us/instruct/darnold/maw/catmap.htm, 1997.
[5] K. Struss, "A Chaotic Image Encryption", In Spring, Mathematics Senior Seminar, Vol. 4901, 2009.
[6] K. Shaw, "Arnold's Cat Map", March 2006.
[7] C. Kuo-Liang and C. Lung-Chun, "Large encrypting binary images with higher security", Pattern Recognition Letters 19, No. 43, Section 4, pp. 461–468, 1998.
[8] S. Li-Ping, Q.G. Zheng, Hong-Jiang and H. Xing-Chen, "2D Triangular Mappings and Their Applications in Scrambling Rectangle Image", Information Technology Journal, 7: 40-47, 2008.
[9] Z. Linhua, L. Xiaofeng and W. Xuebing, "An image encryption approach based on chaotic maps", Chaos, Solitons and Fractals 24 (2004), 759–765, 2005.
[10] S. Mazleena, I. Subariah and F.I. Ismail, "Image Encryption Algorithm Based On Chaotic Mapping", Jurnal Teknologi, 39(D) Dis. 2003: 1–12, 2003.
[11] M. Minati, M. Priyadarsini, M.C. Adhikary. and K. Sunit, "Image Encryption Using Fibonacci-Lucas Transformation", International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.
[12] A.B.Y. Mohammad and J. Aman, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 2008.
[13] A. Musheer and A.M. Shamsher, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2 (1), 46-50, 2009.
[14] S. Al-Maadeed, A. Al-Ali and T. Addalla, "A New Chaos-Based Image-Encrytion and Compression Algorithm". Journal of Electrical and Computer Engineering, Vol. 2012, Article ID 179693, 11 pages, 2012.
[15] Y. Jie, "Algorithm of Image Information Hiding Based on New Anti-Arnold Tranform and Blending in DCT", Department of Communication and Information Engineering, Nanjing Institute of Technology, Nanjing, China.
[16] S. Shekhar, H. Srivastava, and M.K. Dutta, "An Efficient Adaptive Encryption Algorithm for Digital Images", International Journal of Computer and Electrical Engineering, Vol. 4, No. 3, June 2012.

[17] V.A.M. Pemmaraj, "RNS-To-Binary Converter for a New Three-Moduli Set$\{2^{n+1}-1,\ 2^n, 2^n-1\}$", IEEE Transactions On Circuits And Systems—II: Express Briefs, Vol. 54, No. 9, September 2007.
[18] K.A. Gbolagade and S.D. Cotofana, "Residue-to-Decimal Converters for Moduli sets with Common Factors", IEEE, pp. 624-627, 2009
[19] Mi Lu, "Arithmetic and Logic in Computer Systems", John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.
[20] A. Omondi and B. Premkumar, "Residue Number Systems Theory and Implementation", Imperial College Press, 2007.
[21] K.S. Hung, "A Study on Efficient Chaotic Image Encryption Schemes", Rn Run Shaw Library, City University of Hong Kong, 2007.

S. Alhassan, Department of Computer Science, Faculty of Mathematical Sciences, University for Development Studies, Navrongo, Ghana.

Professor K.A. Gbolagade, Department of Computer Science, Faculty of Mathematical Sciences, University for Development Studies, Navrongo, Ghana.