A Novel Lightweight Compact Encryption Algorithm for Embedded Security

SF. Ayesha Takreem[1], T. Sunitha[2]
[1]*M.Tech Scholar, Branch of WMC, G.Narayanamma Institute of Technology & Science, JNTUH, Hyd, India.*
[2]*Assistant Professor, Dept. of ETM, G.Narayanamma Institute of Technology & Science, JNTUH, Hyd, India.*

***Abstract*–**Lightweight cryptography is an interesting field, ideal as a cryptographic algorithm for resource constrained devices that operate using less power and area/space. Lightweight cryptography algorithms aim is in providing higher throughput and compactness utilizing less power and cost without compromising with the security. The lightweight encryption algorithms discussed in this paper are PRESENT-GRP and Chaotic image encryption algorithms. GRP is a bit permutation instruction which is combined with PRESENT which is a substitution-permutation block cipher that combines to produce a novel lightweight encryption algorithm. Drawbacks of PRESENT-GRP algorithm led towards the designing of a new lightweight 1D chaotic image encryption algorithm. The proposed algorithm is a simple, improved and efficient chaotic system developed by taking the difference between the output sequences of the two same existing 1D maps and to reduce the linear-nonlinear conversion to shorten the encryption time. The experimental results show the comparison between the existing and the proposed system representing the better encryption algorithm with the evolution of types of data being shared between devices.

***Keywords*–**PRESENT-GRP, image encryption algorithm, chaotic system, 1D chaotic maps, LLS, SSS.

I. INTRODUCTION

The day to day utilization of pervasive devices[1] for transmitting data across the globe has raised the concern for information security in information communication. These devices deal with irregular phenomena such as illegal copying and misinterpretation of data through illegal/unauthorized personalities and thus the secure utility of data becomes an important issue. In embedded systems, a fully fledged cryptographic system is difficult to be implemented due to the constraints like area, power depletion and cost. All these concerns guide towards using lightweight cryptographic algorithms[2] that operate using less power without compromising with security. There are various variants of lightweight ciphers out of which the best suited for embedded security is PRESENT[3] lightweight block cipher which is a substitution-permutation based network comprising of 80 bit or 128 bit key size and 64 bit block size and performs iterations for upto 31 rounds for one time encryption process. PRESENT algorithm is a secure algorithm which utilizes less memory, space and power and fits best for resource constrained devices such as embedded security, IoT, pervasive devices, etc. The permutation layer of PRESENT algorithm is not as secure as the substitution layer since the permutation layer is mostly subjected to attacks. To increase the strength of PRESENT algorithm, it is combined with a bit permutation instruction set known as GRP (group operation) which is a compact bit permutation instruction set with adequate security and is very complex in nature and comprise of very good diffusion property. Amongst all the bit permutation instructions set, GRP[4] aims to operate using less memory and fast encryption speed compared to the existing permutation instructions. GRP algorithm is able to perform permutation of 64 bit data including control bits within 13 instructions only which means that it is able to provide more security to the data with few instructions (reducing the computational cost) which makes it best suitable for embedded security. PRESENT and GRP algorithms are combined to form a new lightweight cryptographic algorithm that collectively produces an adequate security cryptographic algorithm for embedded security.

The advancement of information technology deals with lots of digital contents(text data, images, videos) been transmitted and stored between devices. The data not only being text data but also digital data needs to be secured across the network.

Digital data such as images differ from normal text data in its intrinsic features such as big size, strong correlation between neighbouring pixels and high redundancy of data. PRESENT-GRP algorithm is suitable for text data but becomes slower while operating with image data. Image data requires strong real-time property with fast encryption speed and high security. One such image encryption algorithm suitable for embedded devices is chaotic image encryption algorithm.

Chaotic image encryption algorithm[5] is a chaos based image encryption algorithm, the system is based on two parts: (i) first part is generation of the security key (ii) performing encryption process using the security key.

The security keys are generated using maps which are categorized into two types: 1-dimensional and multi-dimensional maps, 1D map is easy to implement and have low computational cost making them fit for embedded system application. 1D map exhibit some disadvantages such as limited chaotic behavior range and non-uniform distribution of chaotic sequences output. These parameters led towards proposing an improved 1D chaotic map[6] with increased

chaotic range and behavior. This encryption process reduces the computational time by reducing the linear-nonlinear conversion and therefore gives an influence on the performance of whole encryption system. The analysis and simulation of chaotic map's range expansion possibility is done by using bifurcation map and lyapunov exponent[7]map which demonstrates the accuracy of a chaotic system.

II. LITERATURE SURVEY

PRESENT is a lightweight block cipher with 64 bit block cipher and 80 bit key and is a SP based network. Block ciphers are potentially more capable and compact than stream ciphers, for which it has been aimed to be redesigned to improve the security of the data. PRESENT has been targeted to support the applications which AES couldn't support. The block cipher PRESENT is optimized for performance and space for utilization in resource constrained devices and has fixed key size developed by few manufacturers which rule out any key manipulation attacks for which increasing the key size becomes necessary to reverse any brute-force attacks. For applications demanding more efficient space the block cipher was implemented for encryption only. The design issues for PRESENT algorithm are:

- It provides only moderate security levels with 80 bit key size which has to be extended upto 128 bit keys
- A range of attacks can manipulate the time-memory-data when encrypting large amounts of data, although these attacks are unlikely to be a significant factor

In the recent years there has been many attacks been performed on the permutation layer of security algorithms and PRESENT algorithm's p-layer is not as secure as other algorithms for which it is been combined with other secure and complex bit permutation instruction to form a secure and compact encryption algorithm.

III. PRESENT-GRP HYBRID CRYPTOSYSTEM.

PRESENT-GRP is a compact hybrid cryptosystem that combines the s-box of PRESENT with p-box of GRP which forms a lightweight cryptosystem. The hybrid cryptosystem result in properties which makes them a tinier version than PRESENT algorithm itself.

PRESENT-GRP is a 64/128 bit block with 128 bit key size. Encryption process is performed by first passing the 64/128bit block of plaintext through the s-box of PRESENT after which it is mapped according to the PRESENT algorithm's s-box mapping and then passed through the p-box layer of GRP where, permutation is performed according to GRP's instruction procedure. Key generator produces keys according to GRP at each stage and provides it to the p-layer as shown in Fig.1. The inputs to the GRP key generator are user defined in the form of 0's and 1's. GRP is a very robust and fast bit permutation instructions set which makes it suitable and necessary for such cryptographic algorithm. The bit permutation instruction is able to perform permutations within log(n) steps instead of n steps compared to other bit permutation instructions reducing computational complexity.

PRESENT algorithm contains a non-linear substitution layer, a non linear s-box uses only 4 bits structure which leads to less GE's and power consumption. There are a total of 16 s-boxes of PRESENT which are divided in a group of 4 each.

The hybrid cryptosystem is able to survive brute force attack due to its large key size and is able to resist both linear attacks and differential attacks.

IV. IMAGE ENCRYPTION ALGORITHM

Information security is vital in the day to day life information communication and technology which has been getting advanced globally. With all these advancements lots of digital data is also been transmitted and security of the digital content against irregular phenomena such as misuse or copying of data can lead to impeachment of data and hence protection of this data becomes necessary.

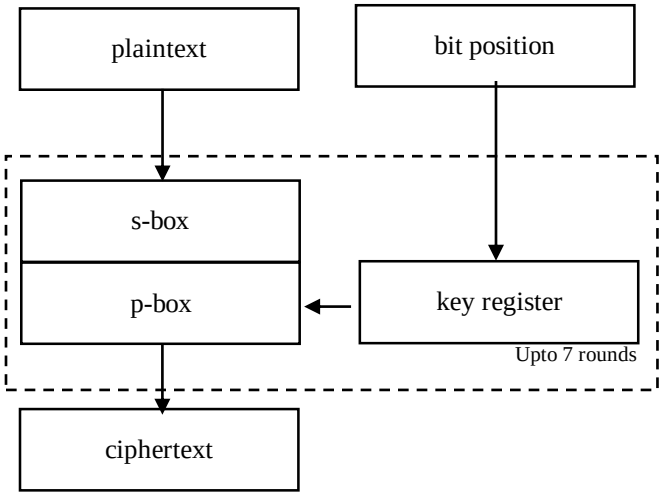


Fig.1: Block diagram of PRESENT-GRP algorithm.

Image data is different from text data in terms of its big size, strong correlation between pixels and high redundancy of data which requires fast speed encryption for real time property in communication. PRESENT-GRP algorithm is suitable for fast cryptography for text data but becomes slower when performing cryptography on image data. For such reason a new image encryption algorithm is used which is also a lightweight encryption algorithm which is a fast and secure encryption algorithm for digital data.

There are a lot of image encryption algorithms such as vector quantization[8], gray code[9], p-Fibonacci transform[10], fractional wavelet transform[11,12], and chaos[13]. Chaotic image encryption algorithm is the most widely used image encryption algorithm due to its speed, security and low computational cost.

V. PROPOSED WORK: CHAOTIC IMAGE ENCRYPTION ALGORITHM

Chaotic image encryption algorithm is a chaos[13] based encryption algorithm that has initial value sensitivity and is a complex cryptographic system. A chaotic image encryption algorithm requires chaotic sequences which are derived through the chaotic maps and this chaotic sequences act as security keys. This security key is able to achieve encryption and decryption effect without being broken. Thus, chaotic encryption algorithm has been used widely in the field of image encryption.

Chaotic image encryption involves two parts; first part is generation of security key and the second part is using the key during encryption process. Security keys are generated through chaotic maps which are categorized into two categories: (a) 1-Dimensional maps and (b) Multi-dimensional maps. Multi-dimensional maps have the disadvantage of complex structures and multiple parameters owing them difficulty in hardware or software implementation which will subject to increase in computational cost making them unsuitable for resource constrained devices.

On the contrary, 1D maps have an advantage of their structure being simple, easy to implement and low computational cost. Besides all these advantages making them fit for lightweight cryptography systems 1D[14] chaotic map has the disadvantage of limited chaotic behavior range and non uniform distribution of output chaotic sequences. These disadvantages motivated to propose a new chaotic map that is able to provide a wider range of chaotic sequences and uniformly distributed output of chaotic sequences. The proposed chaotic maps are able to produce an improved system that reduces the repetition of linear-nonlinear process which would otherwise result in high computational cost.

1. One-Dimensional chaotic map

In this paper two types of chaotic maps are being discussed:

a. Logistic Map

It is a simple dynamic non-linear equation that exhibit complex chaotic behavior and is the most popularly used 1D chaotic map. This can be expressed using the following equation:

$$x_{n+1} = F_L(u, x_n) = u \times x_n \times (1 - x_n) \quad \text{---(1)}$$

where, u is a control sequence within the range of $u \in (0,4]$ and x_n is the chaotic sequence's output and x_0 being the initial value of chaotic map.

The chaotic behavior of chaotic map is represented using bifurcation diagram and lyapunov exponent diagram. The bifurcation diagram[23] represents that the existing chaotic map has the disadvantage of limited chaotic behavior which has its control parameter u is only between [3.57,4] and a chaotic map doesn't exhibit chaotic behavior beyond this range. The lyapunov exponent[15] diagram represents the value for the quantitative evaluation of the chaotic performance. When the graph represents positive values it indicates better chaotic performance and if it's below zero then there is no chaotic behavior.

b. Sine Map

The sine map is a secure and efficient one dimensional chaotic map which is very similar to logistic map in terms of its evaluation results. The bifurcation and lyapunov exponent diagram is similar to that of logistic map except for the range of control sequence. Sine map[16] can be represented using the following equation:

$$x_{n+1} = F_s(r, x_n) = r \times \sin(\pi \times x_n) \quad \text{---(2)}$$

where, control parameter r is within the range of (0,1] and x_n is the chaotic sequence's output.

2. Improved 1-D chaotic map

The previous 1-D maps had the disadvantage of limited chaotic sequence's range and non-uniform distribution of the output of chaotic sequences. The following sections represent the improved versions of chaotic maps.

The new chaotic map is proposed by making a simple and effective chaotic system by using the difference of the two existing outputs of the 1D chaotic map. The maps are a combination of the same existing chaotic maps with improvements in parameters to increase its range, uniform distribution and positive chaotic sequences.

The improved chaotic map is represented using the following equation:

$$x_{n+1} = F(u, x_n, k) = F_{c\square aos}(u, x_n) \times G(k) - floor(F_{c\square aos}(u, x_n) \times G(k)) \quad \text{---(3)}$$

where, $G(k)=2^k$, $8 \le k \le 20$

$F_{chaos}(u,x_n)$ is the previously discussed 1D chaotic maps, $F_{chaos}(u,x_n,k)$ is the newly proposed chaotic map in the extended range and G(k) is an adjustable function with parameter 'k', the larger the value of k the better is its chaotic performance. The floor operation takes input as a real number and gives the output as the greatest integer less than or equal to denoted.

a. Logistic-Logistic map

The improved logistic-logistic map is a combination of two logistic maps which can be expressed using the following equation:

$$x_{n+1} = u \times x_n \times (1 - x_n) \times 2^{14} - floor(u \times x_n \times (1 - x_n) \times 2^{14}) \quad \text{-----(4)}$$

where the control parameter u∈(0,10] and x_0 is the initial value of the sequence. The bifurcation and lyapunov exponent graph describe the chaotic sequences to be improved in both range of chaotic sequence and uniform distribution of output sequences.

b. Sine-Sine map

The sine-sine map is a combination of equation (2) and (3) which can be defined using the following equation:

$$x_{n+1} = u \times sin(\pi \times x_n) \times 2^{14} - floor(u \times sin(\pi \times x_n) \times 2^{14}) \quad \text{---(5)}$$

where the control parameter u ∈(0,10] and x_0 is the initial value of the sequence. The bifurcation and lyapunov exponent graph prove the chaotic sequences to be improved in both range of chaotic sequence and uniform distribution of output sequences. Logistic-Logistic System (LLS) and Sine-Sine System (SSS) have similar bifurcation and lyapunov exponent diagram and show slight variation in the performance. There are many chaotic maps but the best suited for lightweight encryption applications is LLS and SSS.

3. Image encryption process

The proposed new image encryption algorithm is verified for its application in security in the following section. The functioning of the proposed system is explained in the following block diagram. Fig.4 describes the functionality of the proposed cryptosystem that takes the image pixels as an input and performs permutation on the pixels of the image and then these

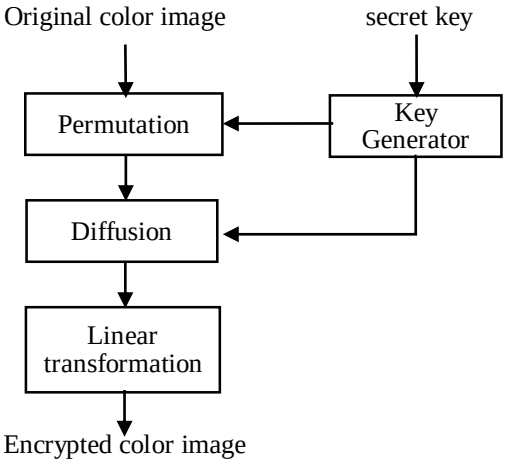


Fig.2: Block diagram of proposed crypto-system

pixels undergo diffusion process and then linear transformation. The key generator generates key and provide it to the permutation and diffusion layer. These keys are generated from the chaotic maps in the form of chaotic sequences. The diffusion process has properties to create complexity in the procedure which makes the system highly sensitive to even a tiny change in the initial conditions giving them an edge in an accuracy of upto 10^{-16} to the initial conditions u and x_0.A slight variation in the initial condition shows a difference in the output.

a. Encryption process

The encryption process requires five parameters which are the security keys (x_0,u,k,N_0,l_p). The image encryption process using 1D chaotic map is done as described in the following steps:

Step 1: The color image of size M×N is converted into gray scale image of size M×3N, if the image is already a grayscale image then there is no need of conversion.

Step 2: The above obtained grayscale image is then converted into a 1D image pixel matrix of size M×3N and the pixel matrix is represented as

$$P=\{p_1,p_2,\ldots p_{M\times 3N}\}$$

Step 3: The chaotic sequence X is obtained from the new proposed chaotic map's equation, where x_0, u and k are the initial values for the chaotic system which are used as security keys. The chaotic system is iterated for N_0 times in order to obtain a new sequence of size M×3N. Where N_0 is also a secret key and is a constant value.

Step 4: The chaotic sequences X obtained from the above procedure are then sorted in ascending order which is expressed as,

$$X'=\{x'_1,x'_2,\ldots x'_{M\times 3N}\}$$

Step 5: These sorted sequences are then permuted. The permuted image position matrix using X′can be expressed as

$$P'=\{p'_1,p'_2,\ldots p'_{M\times 3N}\}$$

Steps 4 and 5 are as shown in Fig.3.The permutation matrix is expressed using the following equation.

$$P'(i)=P(X'(i))$$

Step 6: The diffusion matrix $D'=\{d'_1,d'_2,\ldots d'_{M\times 3N}\}$ is obtained using the following equation.

$$D'(i) = mod(floor((X(i)\times 10^{14}),256)$$

Step 7: The encrypted image pixel $C=\{c_1,c_2,\ldots c_{M\times 3N}\}$ is obtained using D′ and P′ which can be expressed using the following equation.

$$C(i) = mod(P'(i) \oplus D'(i),256) \otimes C(i-1)$$

The process is as shown in Fig.4.

Step 8: The newly encrypted image pixel matrix $C'=\{c'_1,c'_2,\ldots c'_{M\times 3N}\}$ is obtained by rotating the encrypted matrix C to the left by the amount of l_p times, where l_p is also a security key and $l_p \in [1,M\times 3N]$.

This step not only reduces the repetition of linear-nonlinear conversion to shorten the encryption time but also increases the strength of encryption process. This process can be evaluated using the following equation.

$$\begin{cases} C'(i\text{-}l_p)=C(i); & i\text{-}l_p \geq 1 \\ C'((i\text{-}l_p)+M\times 3N)=C(i); & i\text{-}l_p < 1 \end{cases}$$

Step 9: Convert the matrix C′ back to color image of R,G and B with the size of M×3N.

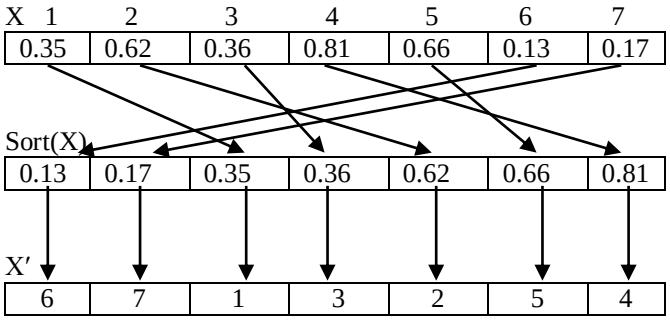


Fig.3: Generation of permuted position Matrix

The diffusion process in 1D chaotic map is as shown in the Fig.4. Cipher data is formed by performing mathematical add operation with permutation and diffusion matrix and then performing MOD operation.

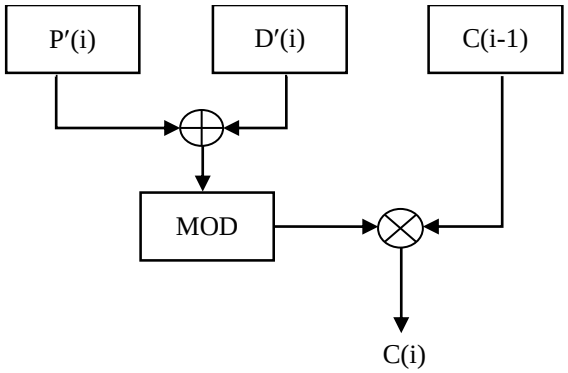


Fig.4: Diffusion process in 1D chaotic image encryption

b. Decryption process

The decryption process is exactly the inverse of encryption process with some slight variation in the diffusion and permutation process which can be expressed with the following equations.

$$P(X'(i)) = P'(i)$$
$$P'(i) = mod(C(i) \otimes C(i\text{-}1) \ominus D'(i), 256)$$

The diffusion process in decryption can be explained with the diagram as shown below. Plaintext data is formed by performing mathematical subtract operation to the ciphertext data and then performing MOD operation.

IV. EXPERIMENTAL RESULTS

The performance evaluation of the encryption algorithm is done using Matlab 2015. The algorithm is evaluated using logistic-logistic system (LLS) map with color images of size

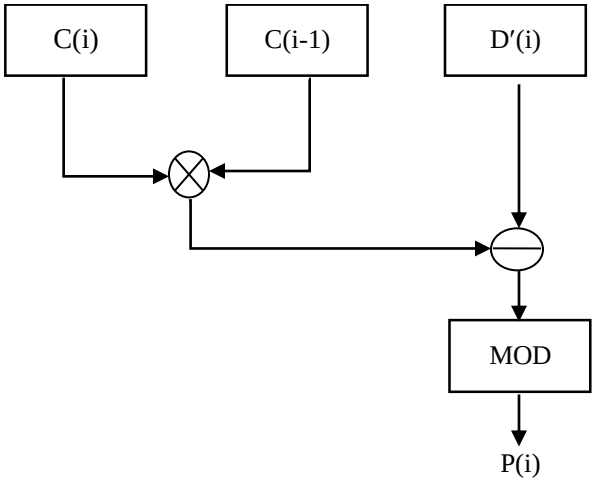


Fig.5: Diffusion process of 1D chaotic image decryption

128×128. The initial condition values of LLS are taken as, the control parameter u=7, k=14, and N_0= 1000. The encrypted and decrypted images are as shown in fig.6.(a) and (c) The images depict that the encrypted images are noise like images and can be effectively applied to images of various forms such as binary images, color images or grayscale images.

1. Security key space

For a security algorithm, the key space should be large enough to resist any key attacks such as brute force attack. An encryption algorithm should have a key space larger than 2^{100} to resist brute force attack. The encryption algorithm should be very sensitive to any change of its security key.

The proposed image encryption algorithm has5 security keys u, x_0, k,$N_0$and l_p, where $u\in(0,10]$, $x_0\in(0,1]$, $k\in$ [8,20] and $l_p\in[1,M\times 3N]$. The initial parameters u and x_0 are set to compute with a sensitivity of upto 10^{-14}, so the total key space that we get is $10^{16}\times10^{16}\times(128\times128\times3)\times 10^3\times12\approx 2^{138}$. This means that the proposed algorithm is able to resist and withheld brute force attack.

2. Statistical analysis

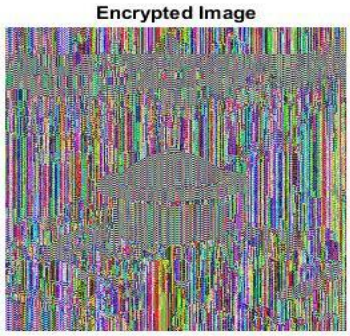
Statistical analysis is one method to evaluate the performance and accuracy of the proposed algorithm.

2.1 Histogram analysis

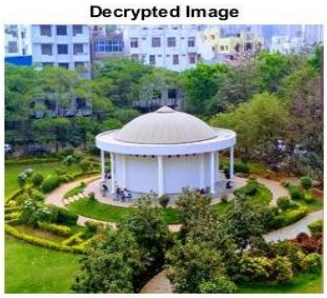
A histogram is the representation of the number of pixels distribution in an image. Hackers try to retrieve data through the statistical distribution of data known as the statistical attack.

To overcome and resist the statistical attack the image histogram should be made flat. The histogram of an image is as shown in Fig.6(d) which represent a uniform distribution of image pixels. The chaotic map used in this encryption process in logistic-logistic system map.

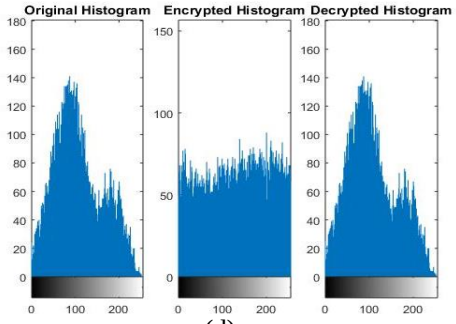
(a)



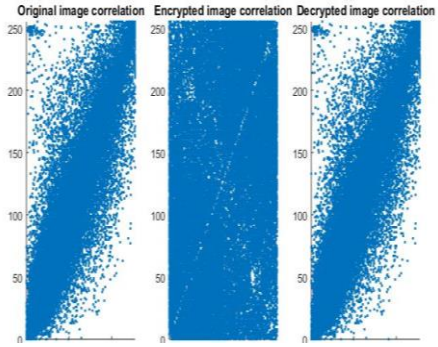
(b)



(c)



(d)



(e)

Fig.6: Encryption and decryption results of an image (a) the original image (b) the encrypted image (c) the decrypted image (d) histogram plot of original, encrypted and decrypted images (e) correlation analysis of original, encrypted and decrypted images.

2.2 Correlation between two adjacent pixels

Image data has its intrinsic data different from normal text data in terms of high redundancy of data, strong correlation between neighbouring pixels that can be used by attackers for attacking information. The correlation plot of an image is as shown in Fig.6(e), the correlation plot is different for different images.

The correlation coefficient is calculated by the following equation.

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

where,

$$cov(x,y) = \frac{1}{N}\sum_{i=0}^{N}\big(x_i - E(x)\big)\big(y_i E(y)\big)$$

$$D(x) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))^2,$$

$$E(x) = \frac{1}{N}\sum_{i=0}^{N} x_i$$

where x and y are the color values of two adjacent pixels of a image. The correlation coefficient of the encrypted images is near to zero or negative values indicating that the encrypted images have no correlation with the original image.

Table 1 Correlation coefficient of encrypted images

Image	Correlation coefficient of encrypted images
Bus.jpg	0.0402
Fruits.jpg	-0.0265
Lena.jpg	0.0028

2.3 Sensitivity analysis

An encryption algorithm should be very sensitive to any tiny differences in the key and plain images. The sensitivity of an algorithm is evaluated using two parameters which are number of pixel change rate (NPCR) and unified average changing intensity (UACI) which are represented using the following equations.

$$NPCR = \frac{1}{M\times N}\sum_{i=0}^{H}\sum_{i=0}^{W} D(i,j)\times 100(\%)$$

where $D(i,j) = \begin{cases} 0 & if\, c_1(i,j) = c_2(i,j) \\ 1 & if\, c_1(i,j) \neq c_2(i,j) \end{cases}$

$$UACI = \frac{1}{M\times N}\sum_{i=0}^{H}\sum_{i=0}^{W}\frac{|c_1(i,j) - c_2(i,j)|}{255}$$

where c_1 and c_2 are encrypted images corresponding to two security keys. The table below shows the NPCR and UACI values for few encrypted images representing their sensitivity with tiny differences in the initial conditions.

Table 2 NPCR values of encrypted images

Image	NPCR(%)		
	R	G	B
Bus.jpg	99.55	99.6	99.62
Fruits.jpg	99.59	99.53	99.57
Lena.jpg	99.7	99.4	99.6

Table 3 UACI values of encrypted images

Image	UACI(%)		
	R	G	B
Bus.jpg	32.65	38.42	38.6
Fruits.jpg	35.44	37	36.4
Lena.jpg	30.5	32	38.9

2.4 Peak Signal to Noise Ratio(PSNR)

Digital images are easily influenced to noise inside the network and in the storage in physical media. An image encryption algorithm should be able to resist such phenomena. To test the ability of this algorithm in the presence of noise it has been tested by adding the image with 3% of salt and pepper noise. After decryption it has been observed that the decrypted image contains most of the data same as the original image even in the presence of noise.

The restoring ability of an image is evaluated with the help of PSNR whose equation is given as,

$$PSNR = 10\times log\frac{255^{\,2}}{MSE}\ (dB)$$

where, $MSE = \frac{1}{M\times N}\sum_{i=0}^{H}\sum_{j=0}^{W}(OI(i,j) - DI(i,j))^2$

where, M×N is the size of the image, 0I(i,j) is the pixel of the original image and DI(i,j) is pixel value of decrypted image.

The larger the value of PSNR, the more difficult it is to distinguish between the original and decrypted image. The larger the PSNR value gets the smaller the breakdown coefficient of the images get.

Table 4 PSNR values of some decrypted images

Image	PSNR value (dB)
Bus.jpg	72.07
Fruits.jpg	43.44
Lena.jpg	46.22

An experimental comparison is done between PRESENT-GRP algorithm and 1D chaotic image encryption algorithm by giving same image as an input to both the algorithms and the performance evaluation result is as shown below in Table 5.

Performance evaluation shows that the proposed image encryption algorithm performs better and the speed of encryption and decryption process is fast compared to PRESENT-GRP algorithm.

Ideally, PSNR value above 35dB is said to be ideal that makes it very difficult to distinguish between original and decrypted images.

The main criterion for opting 1-D chaotic image encryption algorithm over PRESENT-GRP algorithm is the time consumed by the algorithm to encrypt and decrypt an image. 1D chaotic image encryption algorithm not only reduces the computational time but also increases the security of the algorithm.

Table 5 Performance evaluation of PRESENT -GRP algorithm and 1D chaotic image encryption algorithm.

PRESENT-GRP		1D chaotic	
Image	Lena	Image	Lena
Correlation coefficient	0.0784	Correlation Coefficient	- 0.015
NPCR (%)	99.59	NPCR(%)	99.55(R) 99.56(B) 99.58(G)
UACI (%)	14.86	UACI(%)	30.25(R) 32.87(B) 37.04(G)
Time taken to encrypt(sec)	98.89	Time taken to encrypt(sec)	0.94
Time taken to decrypt(sec)	1560	Time taken to decrypt(sec)	75.61

V. CONCLUSION

Information security plays a vital role in information technology that deals with regular transfer of data from one device to another. This data has chances of getting misused by hackers of getting copied or might retrieve any important

information. Embedded devices are resource constrained devices and are a part of daily communication source, security of these devices becomes important.

One such security algorithm is PRESENT-GRP algorithm which is best suited for embedded systems and IoT. This algorithm has the advantage of operating in less memory/space utilizing less power. There are various forms of data such as text data, images, videos, etc are being transferred between the devices and PRESENT-GRP algorithm becomes slow when operating on image data.

Image data is different from text data in terms of redundancy of data, strong correlation between pixels and big size of data. Image data requires strong real time property with fast encryption speed. For such reason a new modified image encryption algorithm is proposed which is fast and secure than block ciphers.

The proposed 1D chaotic image encryption algorithm is designed to be a simple and effective chaotic system. This chaotic system produces a chaotic system which increases the range of chaotic behavior and provides a uniform distribution of the output of chaotic sequence by taking the difference of the output sequences of two same existing 1D chaotic maps. Secondly, the computational time is decreased by reducing the repetition of linear(permutation)-nonlinear(diffusion) conversion, this step not only reduces the computational time but also increases the strength of encryption. Simulation and performance evaluation represented that the proposed system is secure, has excellent performance and is able to resist attacks better than PRESENT-GRP algorithm.

VI. REFERENCES

[1]. A. Poschmann, "Lightweight cryptography: Cryptographic engineering for a pervasive world," Ph.D. dissertation, Faculty of Electrical Engineering and Information Technology, Ruhr-University Bochum, Germany, Feb. 2009.

[2]. T. Eisenbarth and S. Kumar, "A survey of lightweight-cryptography implementations," IEEE Des. Test. Comput., vol. 24, no. 6, pp. 522–533, Nov./Dec. 2007.

[3]. A. Bogdanov et al., "PRESENT—An ultra-lightweight block cipher,"in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4727, P. Paillier and I. Verbauwhede, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 450–466.

[4]. Z. Shi and R. B. Lee, "Bit permutation instructions for accelerating software cryptography," in Proc. IEEE Int. Conf. Appl. Specific Syst., Archit. Process. (ASAP), Jul. 2000, pp. 138–148.

[5]. Y. Sangeetha, S. Meenakshi, CS. Sundaram, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimedia Tools and Applications. 71(3) (2014) 1469-1497.

[6]. Y. Zhou, L. Bao, CLP. Chen, A new 1D chaotic system for image encryption, Signal Processing. 97(7) (2014)172-182.

[7]. C. Lv-Chen, L. Yu-Ling, Q. Sen-Hui, L. Jun-Xiu, A perturbation method to the tent map based on Lyapunov exponent and its application, Chinese Physics B. 24(10) (2015) 78-85.

[8]. TH. Chen, CS. Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Inf. Sci. 180(9) (2010) 16901701.

[9]. Y. Zhou, K. Panetta, S. Agaian, CL. Chen, (n, k, p)-Gray Code for Image Systems, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 43(2) (2012) 515-529.

[10]. Y. Zhou, K. Panetta, S. Agaian, CLP. Chen, Image encryption using P-Fibonacci transform and decomposition, Optics Communications. 285(5) (2012) 594-608.

[11]. S. Li, G. Chen, A. Cheung, B. Bhargava, KT. Lo, On the Design of Perceptual MPEG-Video Encryption Algorithms, IEEE Transactions on Circuits & Systems for Video Technology, 17(2) (2005) 214-223.

[12]. G. Bhatnagar, QMJ.Wu, B. Raman, A New Fractional Random Wavelet Transform for Fingerprint Security, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum.42(1) (2012) 262-275.

[13]. C. Fu, BB. Lin, YS. Miao, X. Liu, JJ. Chen, A novel chaos-based bit-level permutation scheme for digital image encryption, Optics Communications. 284(23) (2011) 5415-5423.

[14]. R. Liu, New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map, Open Cybernetics & Systemics Journal. 9(1) (2015) 210-216.

[15]. MT. Rosenstein JJ. Collins CJD. Luca, A practical method for calculating largest Lyapunov exponents from small data sets, Physica D Nonlinear Phenomena, 65(s 12) (1993) 117-134.

[16]. L. Xu, Z. Li, J. Li, A novel bit-level image encryption algorithm based on chaotic maps.