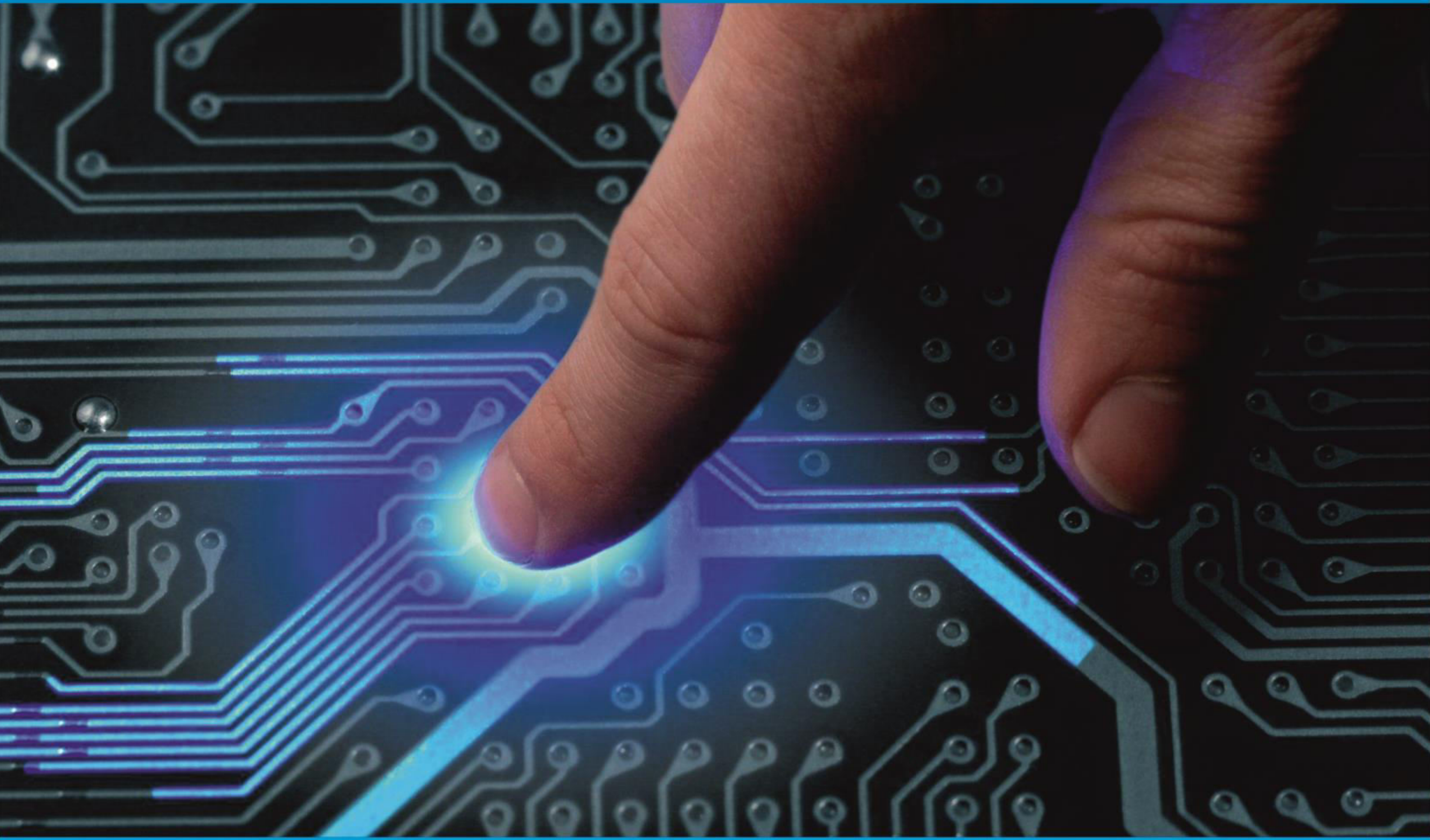
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Text to Image Encryption Using Elliptic Curve Cryptography with Hill Cipher

S.Rajesh Kumar[1,] R.Madhuravani[2], S.Sangeetha[3], M.Surya[4]

Assistant Professor, Department of Electronics and Communication Engineering, Cheran College of Engineering, Tamilnadu, India [1]

UG Student, Department of Electronics and Communication Engineering, Cheran College of Engineering, Tamilnadu, India[2,3,4]

ABSTRACT: Convert text to image is one of the recent approaches used to encrypt text data to colors. One of the more current methods for converting text data to colors is to convert it to a gif. Different methods for implementing this method to shield text data from attackers were suggested by researchers. In order to create a Text-To-Image encryption method, this paper used non-traditional and multi-level replacement and transposition operations. In addition, the suggested procedure makes use of a compound key. To generate the required safe picture, the substitution and transposition operations are implemented in two levels (characters (bytes) and bits) of the text data. Both of these characteristics offer the strategy a lot of advantages when it comes to defending against attackers. The suggested technique was applied and evaluated on a variety of data sets, with the observed findings demonstrating the technique's efficacy and robustness as a Text-To-Image encryption technique. In this scheme, a modern picture encryption technique combining Elliptic Curve Cryptosystem and Hill Cipher (ECC-HC) has been proposed to transform Hill Cipher from a symmetric to an asymmetric technique, increasing its security and reliability while still resisting hackers. Encryption and decryption secret keys are produced using a self-invertible key matrix. In the decryption method, there is no need to find the inverse key matrix. In this paper, a hidden key matrix with dimensions of 44 will be used as an example.

KEYWORDS:- Encryption, Decryption, Hill Cipher, Cryptography and ASCII

I. INTRODUCTION

Cryptography is a mathematical technique for protecting photos from adversaries and increasing the confidentiality of communications. The sender completes encryption to convert the first grayscale picture to a scrambled image before transmitting it across the network to the next recipient (receiver). The collector completes the unscrambling in order to return the figured picture to its original state. Cryptography is divided into two groups: symmetric (private key) and lopsided (public key). In symmetric encryption, the sender uses the same key (private key) for both encryption and decoding, while in lopsided encryption, the sender uses a private key that is distinct from the collector's private key, and each gathering generates the general society and mystery key separately after agreeing on the elliptic Curve space parameters. Both the sender and the receiver are exchanging open keys. One of the most appealing open key cryptography strategies is elliptic curve cryptography (ECC). In comparison to various systems like RSA, ECC aims for a small key size with a small amount of memory and low force. Hill Cipher calculation is one of the symmetric methods; it has high throughput, rapid, and basic structure [1]-[5]. Another encryption scheme is currently being proposed that combines the Elliptic Curve Cryptosystem (ECC) with the Hill Cipher (HC) technique to improve protection and create a new methodology (ECCHC).

The new approach employs ECC to generate the private and open keys, and both the sender and the receiver will then deliver the mystery key without any valid excuse to do so over the internet or via an unbound communications channel. One of the most significant drawbacks of Hill Cipher computation is the lack of a reverse of the main structure. As a result,

The decoding process is impossible if the main lattice is not invertible, and the collector is unable to obtain the first knowledge. This paper avoids this problem by using the self-invertible key structure (the key lattice is self-invertible if [K = K-1]), which reduces the computational procedure needed to process key grid converse during the decoding procedure. For no valid excuse to create the backwards of the key network, both the sender and the receiver build the self-invertible key lattice and use it for encryption and decoding.

Distance gaps in accessing health services have been eliminated by sharing patient data across the phone, thanks to the advent of medical imaging equipment and telemedicine technologies. To protect patients' anonymity, data is secured before being sent over an unstable network. Using a recent discovery in the elliptic curve analogue ElGamal cryptosystem and the Mersenne Twister pseudo-random number generator, the paper proposes an encryption scheme for multiple medical photos. The latest discovery reduces the time it takes to encrypt data and solves the ElGamal cryptosystem's data expansion issue. The proposed encryption algorithm can be used to encrypt multiple medical files, according to simulation, security, and statistical analyses.

Elliptic Curve cryptography is a shared key cryptographic scheme in which the message is encrypted with the sender's private key and decrypted with the sender's public key and receiver's private key. The message is encoded into affine points on the elliptic curve using a modern mapping technique described in this article. The mapping technique transforms plain text into ASCII numbers, which are then converted to HEXADECIMAL. The x and y coordinates are formed by grouping the transformed Hex values together. To prevent security attacks, the converted values are encrypted in reverse order. This approach reduces the overhead of the sender and recipient sharing a similar lookup table. If the group count is odd, it often avoids the additional padding bits, which can be called NULL values [6]-[10].

As privacy violation becomes a big concern in Internet-based purchases, credential systems are gaining in popularity. Private passwords have verification and permission dependent on a user's characteristics rather than the user's name. They also have properties like unlinkability, unforgeability, aversion to property sharing, anonymity, and limited attribute disclosure. In this article, we introduce a private credential scheme that is redefined using elliptic curve cryptography. The modular exponentiation process is reduced to a multiplication operation inside a category using elliptic curve arithmetic. It is decided to use an elliptic curve specified over a prime field Fq. The ECDLREP function, or elliptic curve discrete logarithm representation function, is the foundation of the scheme. As a result, using the versatility of elliptic curve cryptography, this scheme attempts to derive the enticing features of private credentials.

ElGamal is a well-known and widely used cryptosystem. Because of its protection, performance, and low complexity, the elliptic curve algorithm has become a hot topic in the cryptography world. ECC ElGamal encryption algorithm will be improved and its viability and security will be examined using elliptic curve cryptography, combined elliptic curves cryptosystem, and ElGamal algorithm. Finally, two stable data transfer schemes regarding the ECC ElGamal cryptosystem are seen, based on threshold cryptography systems thought [11]-15].

II. RELATED WORK

Public-Key Algorithms are symmetric, which means that the key used to encrypt the message differs from the key used to decode it. The encryption key, often known as the public key, is used to encrypt a file, but only the individual who has the decryption key, often known as the private key, may decrypt it.

Compared to standard symmetric Ciphers, this method of encryption has a range of advantages. It ensures that the receiver will make their public key publicly accessible, and that anybody who wants to give them a message can do so using the algorithm and the recipient's public key. Even if an eavesdropper has the algorithm and the public key, he or she would be unable to decode the document. Only the receiver, who has access to the secret key, is able to decode the letter. Public-key algorithms have the drawback of being more computationally expensive than symmetric algorithms, so encryption and decryption take longer. This does not matter for a quick text message, but it is critical for bulk data encryption. Bob (the recipient) must recognize the key in order to decode a letter. However, Alice (the sender) may have difficulty in informing Bob of the key. Eve may be listening in to their e-mail chat and therefore hear what the key is if they simply settle on a key via e-mail. To address this issue, public key cryptography was created.

Both Alice and Bob have their own key pairs by using public-key cryptography. A public key and a private key make up a key pair. If you encrypt everything using the public key, you will only decode it with the private key. In the same way, if the private-key is used to encrypt anything, it can only be decrypted with the public-key. It is impossible to deduce the private key from the public key alone, or vice versa. This allows Alice and Bob to give their public keys to each other even though the channel they're using isn't safe. Eve now has a backup of the public keys, which isn't a concern. When Alice tries to give Bob a hidden letter, she encrypts it using Bob's public key. The letter is then decrypted by Bob using his private key. Eve can't decipher the message since she doesn't have a backup of Bob's private key. Of course, this ensures Bob must keep his private key under strict lock and key. It is therefore possible for two individuals who have never met to safely share messages using public key cryptography.

III. PROPOSED WORK

Since it can provide high protection with smaller key sizes and lower power consumptions, elliptic curve cryptography (ECC) is a good choice for key creation, encryption, and decryption . An elliptic curve E over a prime field F_p is defined by

$y^2 \equiv x^3+ax+b(\text{mod } p)$

Where $a, b \in F_p$, $p \neq 2,3$, and satisfy the condition

$4a^3 + 27b^2 \neq 0 \pmod{p}$

Hill developed the Hill cipher in 1929, and it is a linear algebra-based polygraphic substitution cipher. Each pixel is measured by a modulo 256 integer. The visibility of a pixel is also indicated by the grey level or grey color in a basic scheme. The lowest degree of grey is 0. Since the highest grey amount of 255 is used, it is an important aspect of the cipher. Each block of n letters (considered an n-component vector) is multiplied by an invertible n n matrix against modulus 256 to encrypt a code. Each block is multiplied by the opposite of the encryption matrix to decode the code. The cipher key is the matrix used for encryption, and it should be selected at random from a collection of invertible n n matrices (modulo256).

Where C = Ciphertext

P = Plain text

K = Self-invertible key

[C] = [P]*[K]mod(256) (for encryption)

$[P] = [C]*[K^{-1}]\text{mod}\ (256)$ (for decryption)

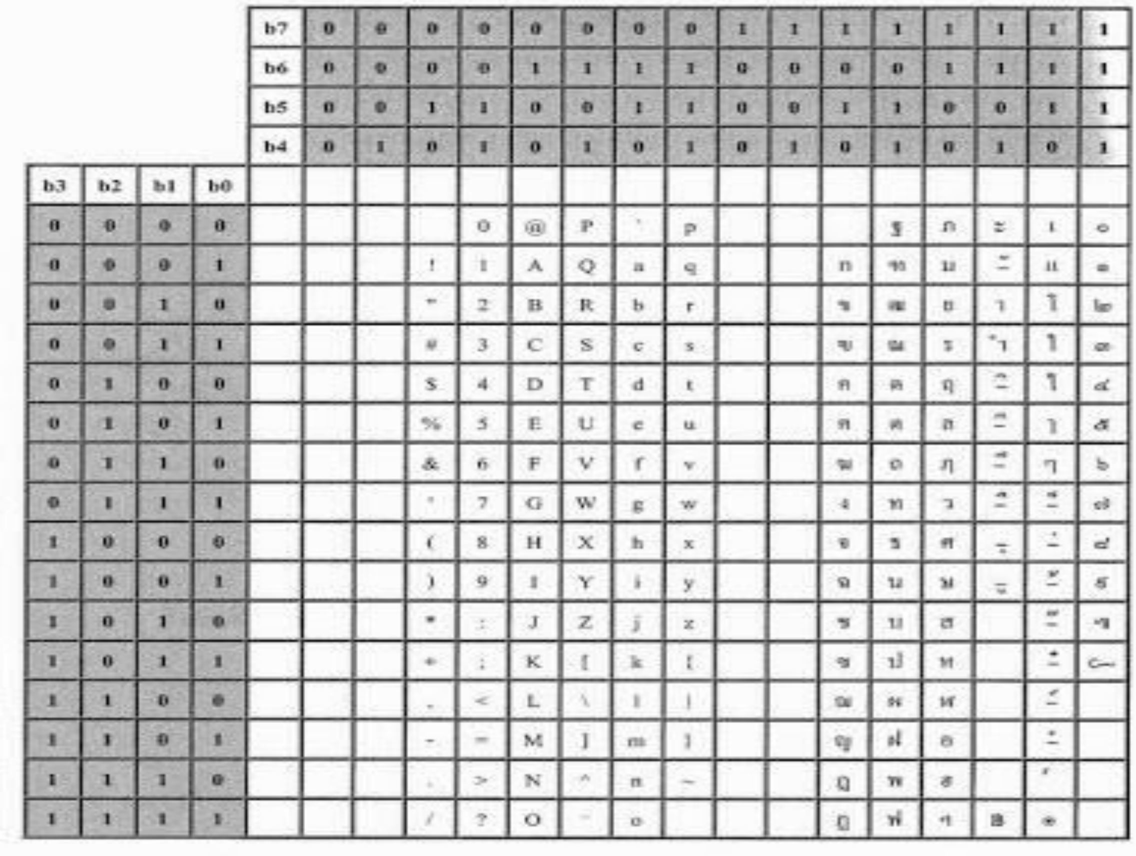
$$[\mathrm{P}] = \begin{bmatrix} \mathrm{P1} \\ \mathrm{P2} \end{bmatrix}, \begin{bmatrix} C1 \\ C2 \end{bmatrix}, [K] = \begin{bmatrix} k11 & k12 \\ k21 & k22 \end{bmatrix} \quad [C] =$$

To decrypt the ciphertext message C , the recipient needs to compute the key inverse (K^{-1}) Where $K*K^{-1}$= I is the identity matrix, then use the following equation to produce the plaintext P

$P= K^{-1}\ C \bmod 256$

Step 1:Text to ASCII conversion

The American Standard Code for Information Exchange, abbreviated as ASCII, is a character encoding standard for electronic correspondence. In computers, telephone equipment, and other instruments, ASCII codes reflect text. While they accept a large number of additional characters, most current character encoding schemes are based on ASCII.



				b7	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
				b6	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
				b5	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
				b4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b3	b2	b1	b0																	
0	0	0	0					0	@	P	`	p				ฐ	ภ	ะ	เ	๐
0	0	0	1				!	1	A	Q	a	q			ก	ฑ	ม	ั	แ	๑
0	0	1	0				"	2	B	R	b	r			ข	ฒ	ย	า	โ	๒
0	0	1	1				#	3	C	S	c	s			ฃ	ณ	ร	ำ	ใ	๓
0	1	0	0				$	4	D	T	d	t			ค	ด	ฤ	ิ	ไ	๔
0	1	0	1				%	5	E	U	e	u			ฅ	ต	ล	ี	ๅ	๕
0	1	1	0				&	6	F	V	f	v			ฆ	ถ	ฦ	ึ	ๆ	๖
0	1	1	1				'	7	G	W	g	w			ง	ท	ว	ื	็	๗
1	0	0	0				(	8	H	X	h	x			จ	ธ	ศ	ุ	่	๘
1	0	0	1				)	9	I	Y	i	y			ฉ	น	ษ	ู	้	๙
1	0	1	0				*	:	J	Z	j	z			ช	บ	ส	ฺ	๊	๚
1	0	1	1				+	;	K	[	k	{			ซ	ป	ห		๋	๛
1	1	0	0				,	<	L	\	l	|			ฌ	ผ	ฬ		์	
1	1	0	1				-	=	M	]	m	}			ญ	ฝ	อ		ํ	
1	1	1	0				.	>	N	^	n	~			ฎ	พ	ฮ		๎	
1	1	1	1				/	?	O	_	o				ฏ	ฟ	ฯ	฿	๏	

Table .1. ASCII Table

The ASCII values are mapped for the corresponding text messages from the above table.

Step 2: ASCII to matrix conversion

Converted ASCII values are stored in a matrix of dimension n×n.

Step 3: Dividing the matrix of n×n into small size of cells of dimension 4×4

Ex;

$$[M]_{16x16}\Rightarrow\begin{bmatrix}\{M1,1\}4x4 & \{M1,2\}4x4 & \{M1,3\}4x4 & \{M1,4\}4x4\\ \{M2,1\}4x4 & \{M2,2\}4x4 & \{M2,3\}4x4 & \{M2,4\}4x4\\ \{M3,1\}4x4 & \{M3,2\}4x4 & \{M3,3\}4x4 & \{M3,4\}4x4\\ \{M4,1\}4x4 & \{M4,2\}4x4 & \{M4,3\}4x4 & \{M4,4\}4x4\end{bmatrix}$$

Where,

$$M_{1,1}=\begin{bmatrix}\mathrm{m}1,1 & \mathrm{m}1,2 & \mathrm{m}1,3 & \mathrm{m}1,4\\ \mathrm{m}2,1 & \mathrm{m}2,2 & \mathrm{m}2,3 & \mathrm{m}2,4\\ \mathrm{m}3,1 & \mathrm{m}3,2 & \mathrm{m}3,3 & \mathrm{m}3,4\\ \mathrm{m}4,1 & \mathrm{m}4,2 & \mathrm{m}4,3 & \mathrm{m}4,4\end{bmatrix}$$

Step 4: Key Generation

User A (The sender)

1. Choose the privatekey $n_a \in [1,e-1]$
2. Compute the publickey $P_a = n_a.G$
3. Compute the initialkey $K_i = n_a.P_b$ $=(x,y)$
4. Compute $K_1 = x.G = (k_{11},k_{12})$ and $K_2 = y.G = (k_{21},k_{22})$
5. Generate the self-invertible key matrix K_m

User B (The receiver)

1. Choose the private key $n_b \in [1,e-1]$
2. Compute the public key $P_b = n_b.G$
3. Compute the initial key $K_i = n_b . P_a =(x,y)$
4. Compute $K_1 = x.G = (k_{11},k_{12})$ and $K_2 = y.G = (k_{21},k_{22})$
5. Generate the self-invertible key matrix K_m

Step 5: Encryption (User A)

1. Take cells in the matrix.
2. Arrange each block into cells of size (4x4).
3. Multiply the self-invertible key matrix K_m with each Cells in the matrix ($M_{1,1}$,$M_{1,2}$,$M_{1,3}$ …$M_{1,6}$) and take modulo 256 for each value
$C_{1,1} = (K_m . M_{1,1}) \bmod 256$.

4. Construct the ciphered image C from the values in the ciphered cells ($C_{1,1}$,$C_{1,2}$,$C_{1,3}$ …$C_{1,4}$).

Step 6: Decryption (User B)

1. Separate the ciphered image pixel values into cells of size4x4.
2. Multiply the self-invertible key matrix K_m with each Cells in the matrix ($C_{1,1}$,$C_{1,2}$,$C_{1,3}$, $C_{1,4}$) and take modulo 256 for each value
$D_{1,1} = (K_m . C_{1,1}) \bmod 256$.
3. Construct the Deciphered matrix D from the values in the deciphered cells ($D_{1,1}$,$D_{1,2}$,$D_{1,3}$, $D_{1,4}$).

IV. RESULTS AND DISCUSSION

This method was created in MATLAB 2014a, and the results were evaluated and compared to other schemes to show that our scheme is effective. The suggested system is more effective than other systems, according to our findings.

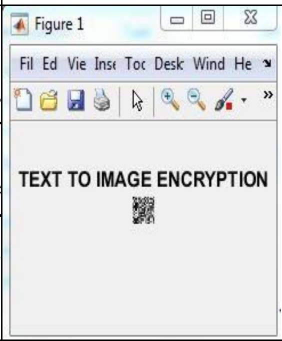
ORGINAL TEXT	ENCRYPTED IMAGE	DECRYPTED TEXT
A musical chord may be represented as the intensity or loudness of its constituent notes using the Fourier transform, which decomposes a signal as a function of time into the frequencies that make it up. The Fourier transform theorem is crucial in implementations.	 TEXT TO IMAGE ENCRYPTION	A musical chord can be represented as the intensity or loudness of its constituent notes using the Fourier transform, which decomposes a function of time into the frequencies that make it up. The Fourier transform theorem is extremely important in implementations.

Table.2 Examples of encrypted and decrypted Images

The quantity used to measure picture ambiguity is information entropy. It will have a certain amount of disarray. The entropy grows and the structure becomes less predictable as the degree of disorder grows.

The entropy is given as,

$$E = \sum_{i=0}^{n} P(x) \times \log_2 P(x)$$

Where, x represent the test image, x_i symbolize the i_{th} possible value in x. Entropy of encrypted images using our algorithm and other references are shown in Table.

Image Name	Our approach	Ref 3	Ref 4	Ref 5	Ref 6	Expected Value
Lena	7.9957	7.9961	7.9972	7.9976	7.9891	8

Table.3. Entropy Values for Scheme and Reference

The theoretical entropy value for a gray scale image is 8 and it is expected to be near to 8. The entropy value calculated for our algorithm is 7.9963.

V. CONCLUSION

The encryption algorithm is implemented using an updated hill cipher method in this proposed system, and one reference picture, Lena, was tested using MATLAB2014a. With different schemes, various output parameters were

| DOI: 10.15680/IJIRCCE.2021.0903184 |

measured and evaluated. Our proposed image encryption algorithm is successful, as evidenced by the entropy value of 7.9957 for the cipher image. The SSIM value of 1 indicates that the initial and decrypted images are identical and that no errors occurred during the encryption and decryption processes. Other efficiency parameters measured for our proposed algorithm, such as MSE, PSNR, and UACI, indicate that our current proposed scheme is more effective and reliable for picture encryption.

REFERENCES

[1] ZiadE.Dawahdeh, ShahrulN.Yaakob, RozmieRazif bin Othman, A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher, Journal of King Saud University - Computer and Information Sciences, (2017). https://doi.org/10.1016/j.jksuci.2017.06.004.

[2] HossamDiab, Aly M. Elsemary, Secure Image Cryptosystem with Unique Key Streams viaHyper-chaotic System, Signal Processing, (2017).doi:10.1016/j.sigpro.2017.06.028.

[3] Naveen Kumar S K, Panduranga H ,TAdvanced Partial Image Encryption using Two-Stage Hill Cipher TechniqueInternational Journal of Computer Applications (0975 – 8887) Volume 60– No.16, December 2012

[4] Wang, Xingyuan& Wang, Qian& Zhang, Ying-Qian. (2014). A fast image algorithm based on rows and columns switch. Nonlinear Dynamics. 79. 1141-1149. 10.1007/s11071-014-1729-y.

WenhaoLiu, KehuiSun ,CongxuZhu: A fast image encryption algorithmbasedon chaotic map. OpticsandLasersinEngineering10.1016/J.OPTLASENG.2016.03.019

[5] XiaoChenab,Chun-JieHua,Adaptive medical image encryption algorithm based on multiple chaotic (2017) https://doi.org/10.1016/j.sjbs.2017.11.023

[6] Congxu Zhu, A novel image encryption scheme based on improved hyper-chaotic sequences, Optics Communications 285 (1) (2012) 29—37.doi:10.1016/j.optcom.2011.08.079.

[7] Xiao, Chun-Jie Hu, Adaptive medical image encryption algorithm based on multiple chaotic Mapping, Saudi Journal of Biological Sciences 24 (2017)1821–1827.

[8] Deng, S.J., Huang, G.C., Chen, Z.J., 2011. Research and implement of Self adaptiveimage encryption algorithm based on chaos. J. Comput. Appl. 31 (6),1502–1504.

[9] Zhang, J., Hou, D., Ren, H., 2016. Image Encryption Algorithm Based on DynamicDNA Coding and Chen's Hyperchaotic System, Mathematical Problems inEngineering, Article ID 6408741,11pages.

[10] ZhongyunHua, Fan Jin, BinxuanXu, Hejiao Huang, 2D Logistic-Sine-Coupling Map for Image Encryption, Signal Processing (2018), doi:10.1016/j.sigpro.2018.03.010.

[11] Hui Wang, Di Xiao, Xin Chen, Hongyu Huang, Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map, Signal Processing (2017), doi: 10.1016/j.sigpro.2017.11.005.

[12] RushiLan, Jinwen He, Shouhua Wang, TianlongGu, XiaonanLuo, Integrated Chaotic Systems for Image Encryption, Signal Processing (2018), doi:10.1016/j.sigpro.2018.01.026.

[13] SakshiDhall , Saibal K. Pal , Kapil Sharma , Cryptanalysis of image encryption scheme based on a new 1D chaotic system, Signal Processing (2017), doi:10.1016/j.sigpro.2017.12.021.

[14] ZhongyunHua, Shuang Yi, Yicong Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Processing (2017), doi:10.1016/j.sigpro.2017.10.004.

[15] M. Li, Y. Guo, J. Huang, Y. Li, Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure, Signal Processing: Image Communication (2018), https://doi.org/10.1016/j.image.2018.01.002

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details