



ENHANCING SECURITY IN CRYPTOGRAPHIC SMART CARDS THROUGH ELLIPTIC CURVE CRYPTOGRAPHY AND OPTIMIZED MODIFIED MATRIX ENCODING ALGORITHMS

¹G.PRAKASH, ² Dr. M.KANNAN

¹Research Scholar, Information and Communication Engineering, Anna University, Chennai

¹Associate Professor, Department of Information Technology, Sona College of Technology, TPTC Main Road, Salem – 636005, TamilNadu, India

²Professor, Department of Information Technology,

Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India.

E-mail: ¹gprakas74.h@gmail.com, gprakash0673@gmail.com, ²kannankrish68@yahoo.com

ABSTRACT

Now-a-days Cryptographic smart cards are being used for most of the online transactions in many fields. But the security and the privacy of usage of these smart cards have been threatened by various attacks to hack the passwords of the smart card users. Since, small length passwords are easily accessible to hackers, users and organizations adapt to longer passwords or to change their passwords frequently. But the risk of having longer passwords or changing passwords frequently is that the passwords could be easily forgotten. Researchers have got this into their main concern and have worked on improving the security of these Cryptographic smart cards. They have employed several cryptographic techniques to embed the card holder details and the password into the smart card. However, those methods invented to improve the smart card security are not up to the requirements. In this work, we have designed a secure technique by integrating both Cryptography and Steganography which can be used for Smart Card Security. Initially, user's confidential details are encrypted using the most secure Elliptic Curve Cryptography (ECC) technique and then the encrypted cipher is embedded into the users photographic image using a novel proposed steganographic technique named Optimized Modified Matrix Encoding (OMME) algorithm. While embedding the encrypted user details into the image of the user, in order to reduce distortion of stego-image, an Optimization algorithm, Artificial Bee Colony (ABC) technique is used to select the image pixels where the secret data should be embedded. On the other end, the secret data embedded into users' image is extracted and it is de-ciphered. If the match occurs, then user will be authenticated. This proposed technique increases the level of security and thus it can be used for the security of smartcards when compared to existing methodologies, since ECC is more secure than any other cryptographic algorithm and the modified matrix encoding using ABC algorithm embeds more number of message bits and simultaneously reduces distortion in stego image.

Keywords: *Elliptic Curve Cryptography (ECC), Optimized Modified Matrix Encoding (OMME), Artificial Bee Colony (ABC)*

1. INTRODUCTION

Today's applications require more functionality and security and are much more complex. Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" governs an extremely wide range of applications and touches everyone's daily life. Concerns over data security are at an all-time high, due to the rapid advancement of technology into virtually every transaction, from parking meters to

national defense. The security field uses three different types of authentication: (i) a password, PIN, or piece of personal information (ii) a card key, smart card, or token (like a SecureID card); and (iii) a biometric [1]. A smart card, a type of chip card, is a plastic card embedded with a computer chip that stores and transacts data. This data is associated with either value or material or both and is stored and processed within the card's chip, in the memory of a microprocessor [2]. France was the nation to invent smart card technology earlier, but because of its limited technical infrastructures and



as it was expensive, consumers were not interested to adopt these cards. These cards provided only limited capability to store the user's personal information securely [3]. To ensure the development of smart card technology, it is necessary that the users must be made to trust that their personal information's are not passed on to third parties. It could be ensured by the use of formal techniques for the specification and verification of smart card applications [4]. The smart cards used in early days were limited to mechanisms that prevented the card from being filled up again. Today's smart cards are reusable, holds large amount of data with high transaction rates. These smart cards are equipped with microprocessors which are capable of performing on-card operations [5]. It can provide identification, authentication, data storage and application processing.

The smart cards are very useful in the commercial security world, because most of them are developed with cryptographic tools. Smart cards have the remarkable benefits over their magnetic-stripe associates of being able to execute cryptographic algorithms in their internal circuitry. This means that the user's secrets (be these PIN codes or keys) never have to leave the boundaries of the tamper-resistant silicon chip, which brings maximum security to the overall system in which the cards participate [6]. Some of the domains that are currently using smart cards are, telecommunication industry, banking industry for credit cards and debit cards, healthcare domain, audiovisual industry, identification industry, transportation industry, access control industry etc [7]. These cards are built-up with cryptographic computations based on secret keys embedded in their non-volatile memories. Usually the attacks on smart cards are performed to extract these secret keys from the tamper resistant card in order to modify the contents in the card and perform an authorized transaction [8]. An authentication technique would be more effective in such cases. An authenticated smart card operates only when a PIN is fed. After authentication, the smart card signs a time-stamped certificate to delegate a part of user's authority for a particular time period [9]. There are many password authentication schemes. A remote password authentication scheme used in remote networks is also a password authentication scheme. In remote password authentication schemes, the communication links among login points and the system are long and insecure [10].

The password guessing attack can be classified into online and offline password guessing attack. The attacker uses the guessed passwords iteratively to pass the verification of the server in an online manner in online password guessing attack. While in offline password attack, the attacker intercepts some password-related messages exchanged between the user and the server, and then iteratively guesses the user's password and verifies whether his guess is correct or not in an offline manner [11]. Particular attention is needed when security is asked to be adaptive and when privacy is asked to be preserved. Adaptivity requires flexible procedures of control being able to react to situational changes in a non-intrusive way [12].

Logical attacks on smart cards focuses on different aspects of potential logical flaws that exists on the Hidden Commands, Parameter Poisoning and Buffer Overflow, File Access, Malicious applets, Communication Protocol, Weak Cryptographic protocols. Side-Channel attacks on smart cards represent the attacks which observe the behavior and characteristics of the smart card transactions through various parameters like power consumption, electromagnetic radiation, time, and voltage. Hence, the basic functionality of Cryptographic Smart card security system is being considered obsolete. Based on the above details, it was very clear that any smart card security system is breakable. However, there is usually an estimate for the cost required to break the system, which should be much lesser than the value of the data being protected by the system [13].

The combination of a smart card and a PIN (either represents a secret key or password) provides Two-Factor Authentication, where two items are needed: something physical the user has (a smart card) and something the user knows (a PIN). Since something physical and something non-physical are both required, the result is a much more secure means of authenticating users. Logins based on usernames and passwords are not as secure as Two - Factor Authentication since usernames are easily determined — they are essentially single-factor authentication (i.e. something you know — the password or personal identification number (PIN)).

Two-factor authentication offers identity theft protection by making it difficult for attackers to steal users' online identities. Two-factor authentication requires the user to physically possess something in addition to something the user knows [14]. Generally speaking, two-factor authentication protocols should consist of



registration, login and verification phases. The user and server share a secret, which is stored in the user smartcard, by combining it with the user password in the registration phase [15] [16]. The remaining section of this paper describes about the works related to smart card security and the proposed system.

2. RELATED WORK

I-En Liao *et al.* [17] have presented a new password authentication scheme to solve the problem of password authentication in insecure networks. This scheme employs some basic concepts, such as one-way hash function, e.g., MD5, or SHA-1, discrete logarithm problem, and Diffie-Hellman key agreement protocol. The security of this scheme is based on having both the properties of discrete logarithm problem and secured one-way hash function. This scheme does not add too much computational complexity. In this scheme instead of having verification table for storing encrypted user password the server keeps only one secret key 'x' known and maintained by the server. This scheme is a better approach and its primary merit is in its simplicity and practicality for implementation under insecure networks. But if the secret key is known to others, this scheme is destroyed.

Rajaram Ramasamy *et al.* [18] have proposed a password authentication scheme for smart card using RSA. In this scheme, the login request for the user was generated based on password, current time and user's secret information. The server does not maintain any password table and instead it maintains only the registration time for every user. This scheme also restricts well-known attacks with a reasonable computational cost.

Yadholla Eslami *et al.* [19] have proposed a hardware implementation of three standard cryptography algorithms on a universal architecture. The micro-coded cryptography processor targets smart card applications and implements both private key and public key algorithms such as DES, AES and ECC in terms of simple logical operations and also meets the power and performance specifications.

Sandeep Kumar Sood [20] has proposed a new dynamic identity based authentication scheme that uses the nonce and timestamp at the same time to resolve the problem of stolen smart card attack keeping the merits of Liu *et al.*'s scheme which is a nonce based mutual authentication scheme using smart cards. In the proposed protocol, the

communication cost of authentication includes the capacity of transmitting message involved in the authentication scheme.

Manoj Kumar [21] has proposed an enhanced remote user authentication scheme with smart card that not only resolves all the security problems of Hwang and Li's scheme, but also adds mutual authentication, session key generation and password change phase and provides forward secrecy to the long term secret key of the remote server. In this scheme, the server and user authenticate one another and then generate a secret session key for secure communication. Also, the remote user is free to change his/her password without connecting to server.

YongSoo Choi *et al.* [22] have proposed an improved modified matrix encoding technique on steganography. They proposed this technique to improve the quality of the stego image by reducing the amount of distortion that occurs while applying the steganographic method to the image in compressed domain. They concentrated on the quantization table to reduce the distortion of the image in compressed domain, while the previous techniques were concentrating on the change of the coefficients to hide the data and then reduce the distortion. The Modified Matrix Encoding algorithm (MME) reduces the degradation occurring during embedding process of the JPEG coefficients. But their proposed technique proved that, there is some more possibility to reduce the distortion by making changes to MME. Here, they have considered the effect of the quantization table while modifying the JPEG coefficients. The experimental results of their proposed technique has shown that considering the quantization factor's effectiveness rather than considering the error from modifying coefficients results in stego object with high image quality.

S. Brindha *et al.* [23] have proposed a LSB steganographic technique based smart card authentication system in which the finger print image of the user is hidden in the face image of the user. This system had used an encryption technique and a steganographic technique. They have used a 24 bit colour image as the cover image. The fingerprint image of the user is encrypted along with the password provided by the user using an encryption algorithm before embedding it into the cover image. Then the encrypted finger print image is embedded into the cover image by using a Scattered LSB steganography method, which modifies the least significant bits of the cover image. But this technique did not embed the

fingerprint image bits linearly. Instead the encrypted fingerprint images were embedded into the cover image bits based on Pseudo Random Number Generator (PRNG). The values of the PRNG were based on the password provided by the user. The performance of this scattered LSB technique was compared with the performance of ordinary LSB technique in terms of PSNR values of the stego image.

Olaniyi, O. M *et al.* [24] have proposed a secured electronic voting system based on an improved stegano-cryptographic model. In their work they have presented the application of both cryptography and steganography to develop an improved model for secure remote electronic voting system. They have used a general private key cryptographic and LSB steganographic technique in their work. The vote of the voter is the secret message and it is embedded into the cover image. This work resulted in a hybrid model by the introduction of a stego key. The receiver can extract the secret message from the cover media only with the help of the stego key. They have implemented their proposed model on a client-server based architecture model which is three-tier architecture.

H S Manjunatha Reddy *et al.* [25] have proposed a wavelet based non LSB steganography. In this work they have initially segmented the cover image into 4x4 cells. Then DWT was applied to these 4x4 cells. Among that, they have considered the 2x2 cells of the HH band of DWT. These cells were manipulated with a payload bit pairs using identity matrix to generate stego image. The payload bit is extracted using key in the destination. This wavelet based non LSB steganography technique was proved to be robust since the payload bit is embedded into the cover image indirectly. Also the PSNR values are high when steganography is done using IWT when compared to steganography performed by DWT.

3. PROPOSED SYSTEM

The smart cards are embedded with integrated circuit (IC) chips, mostly microprocessors which are capable of storing data and at the same time they can perform operations using the data stored in these cards. Most of the manufacturer's design their smart cards with microprocessor chips having inbuilt encryption techniques like DES, 3DES and RSA. But as mentioned above, those cryptographic algorithms are vulnerable to attacks of hackers and intruders. So an alternate mechanism combining a more effective encryption technique and a steganographic technique is proposed here. This proposed technique provides a two factor authentication where the first factor lies in encrypting the user details using ECC and the second factor of authentication lies in embedding the encrypted cipher into the digital photographic image of user using optimized modified matrix encoding steganographic technique. Then at the terminal end, the hidden message is extracted from the digital photographic image of the user and decrypted. Only if both image and user details are matched, the user is authenticated and granted permission to perform required operations.

The trigger for implementing this technique to be used in smart card by integrating both cryptographic and steganographic technique were the attacks made on cryptographic smart cards. The main vantage of using steganography is that the hidden information is not known to naked eyes. Also since the microprocessor embedded in smart cards can perform operations on the data stored on it, both cryptography and steganography are used for additional levels of security. This proposed system consists of two main operations, the first one is encryption of secret data using Elliptic Curve Cryptography (ECC) and the second part is hiding the encrypted cipher into digital photo image using optimized modified matrix encoding steganography technique. The structure of proposed novel technique is illustrated in Figure. 1.

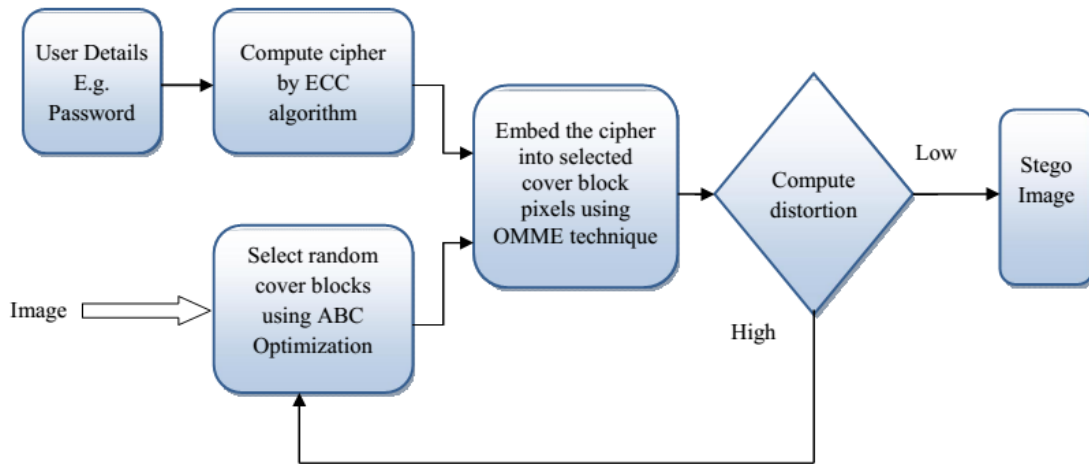


Figure 1: Structure Of Proposed Secure Smart Card Using ECC And Optimized Modified Matrix Encoding Technique

Initially, the users' data is encrypted using ECC algorithm to obtain the cipher. By applying ECC algorithm over a prime field F_p , an encrypted cipher is obtained. Later this cipher is embedded into users digital photographic image using an optimized modified matrix encoding steganographic algorithm. The modified matrix encoding steganographic technique is optimized using Artificial Bee Colony (ABC) optimization algorithm. Initially this modified matrix encoding technique assumes to modify all the image pixels of digital photograph to embed the encrypted cipher. When all cipher is embedded into all image pixels, the distortion in the stego image will be high. So to reduce distortion, the optimal image pixels are selected to embed cipher using ABC optimization algorithm.

3.1. Elliptic Curve Cryptography (ECC)

Initial process in this technique is encrypting the user details along with their password using an effective cryptographic algorithm. Here, encryption of the user's secret data is done using the most secure Elliptic Curve Cryptography (ECC) algorithm. The efficiency of a cryptographic algorithm is based on the complex mathematical operations it performs which are not easy to solve. ECC is a public key cryptographic algorithm where the cryptographic operations are described over an elliptic curve $y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$. Based on the values of a and b different elliptic curves are generated and all the points (x, y) that satisfy the above equations lie on the elliptic curve.

Public key cryptography is a cryptographic system where all users taking part in the communication makes use of a public key and a private key. Only the public key is known to all users and private key

is known only by that particular user. In ECC the public key is any point on the curve and it is obtained by multiplying generator point G along with private key. Private key is any random number.

As mentioned above, the security and secrecy of a cryptographic algorithm lies in the complex mathematical operations it performs. Similarly the efficiency of ECC lies in elliptic curve Discrete Logarithm Problem. The main operation of ECC is point multiplication which involves both point addition and point doubling.

3.1.1. ECC over a Prime Field F_p

By foundation, the elliptical curve operations are very slow. But a cryptographic algorithm must be fast in computation to make it more efficient. So, the operations of the elliptic curve cryptographic algorithm are defined over two finite fields (i) Prime Field and (ii) Binary Field. For our implementation, we have used the ECC over prime field F_p . The equation for elliptic curve over F_p is given by eq (1).

$$y^2 \text{ mod } p = x^3 + ax + b \tag{1}$$

where,

$$4a^3 + 27b^2 \text{ mod } p \neq 0 \tag{2}$$

and the value of p is chosen such that there are large number of points on the elliptic curve to make the cryptographic algorithm more secure.

A. Point Multiplication:

The point multiplication is the main operation of ECC algorithm. In this operation, a point on the curve is multiplied with another scalar value to obtain a new point.

$$kp = Q \quad (3)$$

where k is the scalar and P is a point on the curve. This point multiplication can be achieved only by performing two other main operations namely the point addition and point doubling.

B. Point Addition:

Point addition is the process of adding two points on the elliptic curve to obtain another point on the same elliptic curve. Let J and K be two points on elliptic curve. These two points are added to obtain another point L on the same elliptic curve.

$$L = J + K \quad (4)$$

C. Point Doubling:

In point doubling, a point on the elliptic curve is added to itself to obtain another point on the same elliptic curve. Let J be a point on the elliptic curve, and it is added to itself in order to obtain another point L on the elliptic curve. It is given by,

$$L = 2J \quad (5)$$

In ECC over prime field, the elements of the prime field are the numbers between 0 and $p-1$. Also the domain parameters for this ECC over prime field F_p constitute the coordinates a , b , generator point G , prime number p and the order of elliptic curve n . The main advantage of using this ECC as the cryptographic algorithm is its key size which is small and constant. A 160 bit key used in ECC is considered to be as strong as 1024 bit key used in RSA cryptographic algorithm.

3.1.2. Encryption via Elliptic Curve Cryptography (ECC)

This section briefs about the process of encrypting user information using elliptic curve cryptography. In ECC, we randomly select a basic point P_i that satisfies eq.1 mentioned in previous section. To perform encryption on the given message (eg. Password), we need to select a private key P_k which is a randomly selected integer less than N and we generate a public key $u_k = P_k * P_i$.

Cipher Generation: The steps involved in generating the cipher are,

❖ Choose a random integer k from N ($k < N$), k is a prime number)

❖ Calculate $cg_l = k(m_l - p_k * x_j)$; here m_l represents the message bit and l is the number of characters in the message. (6)

❖ Compute $(x_j, y_j) = p_k * (x_i, y_i)$ (7)

❖ Generate secret message $s_m = (m_l, x_j, y_j, cg_l)$, If size s_m is not equal i.e., $s(m_l) \neq s(x_j) \neq s(y_j) \neq s(cg_l)$, then append zeros to the actual value.

3.2. Optimized Modified Matrix Encoding (Data hiding technique)

For this proposed technique, to embed the cipher into the users' digital photographic image, an optimized modified matrix encoding data hiding technique is used. Usually in modified matrix encoding technique, all the pixels of the image are modified with secret data. Because of this, a lot of distortion occurs in resulting stego-image, which could be easily detected by Steganalysis. Hence, selected pixels must be used to embed the cipher text into cover image. For this selection of pixels, ABC optimization algorithm is used. By using this technique, the system assumes to embed the cipher into different pixels of cover image and selects the pixels where the distortion is low. The following section describes the ABC algorithm and Modified Matrix Encoding technique.

3.2.1. Artificial Bee Colony (ABC) Optimization Algorithm

The Artificial Bee Colony (ABC) algorithm is a swarm optimization algorithm which is based on the behavior of honey bee. In ABC algorithm, three kinds of bees are involved.

- Employed Bee
- Onlooker Bee
- Scout Bee

Among these, the employed bees are the worker bees and both onlooker bees and scout bees are unemployed bees. The steps of functioning of ABC algorithm is given below.

- **Initial food sources are assigned to each employed bee.**
- **Repeat**
 - **Employed Bees Phase**
 - Each employed bee finds the food source allocated to it and registers the nectar amount in that food source.
 - Calculates the fitness value of the food source.
 - **Onlooker Bees Phase**
 - Depending on the waggle dance performed by the employed bee an onlooker bee selects its food source and finds the neighborhood of that food source.
 - Find the nectar amount in the neighbor food source and calculate its fitness value.



- *Compares the fitness of both the food sources and selects the food source with best fitness value.*
- **Scout Bee Phase**
- *It selects a food source randomly based on the onlooker bees selection*
- *Food sources that cannot be improved are neglected or abandoned.*
- **Memorize the best food source.**
- **Until (Requirements are met).**

Similarly, to select the best pixels from the cover image for embedding the secret value (eg. PIN, Passwords, Private keys), optimization using the ABC technique is deployed in the modified matrix encoding algorithm. Instead of food sources, it selects the pixel values in digital image and makes changes by embedding the cipher and then tests for distortion. The algorithm is repeated until an embedding with less distortion is gained.

3.2.2. Modified Matrix Encoding

The Modified Matrix Encoding technique is the steganographic algorithm which implements matrix encoding. F5 steganographic algorithm [26] was the first steganographic algorithm to implement matrix encoding. In F5 steganography, there are two steps.

- i. Permutative Straddling
- ii. Matrix Encoding

In permutative straddling, initially the image pixels are shuffled using a permutation which depends on a key. Then it performs matrix encoding on the shuffled pixels and after encoding, the pixels are rearranged based on the permutation sequence.

This matrix encoding makes use of (1,n,k) encoding to embed k number of secret bits into n number of cover block bits by changing one bit position. The bit position *b* to be changed in cover block CB is found by,

$$b = MB_{bit} \oplus CB_{bit} \quad (8)$$

If the value of *b* is 0, then there is no need to change any bit position in the cover block. Else the bit position *b* in the cover block is changed either from 0 to 1 or from 1 to 0.

In modified matrix encoding technique, instead of (1,n,k) we make use of (t,n,k) where the value of t=2. In this technique, k numbers of message block (MB) bits are embedded into n number of bits of the cover image blocks by changing two bits of the cover block CB. This increases the choice of selecting the bits to be changed. In F5 matrix encoding, the bit position *b* in cover block will be changed. In modified matrix encoding, the bit *b*

selects a pair of values α and β such that $a \oplus \beta = b$.

Let EB be the embedded block, and if the value of *b* is 0 there is no need to change the cover block. Else the bit positions α and β of the cover block are changed based on the ABC optimized bit positions.

$$EB = \begin{cases} CB, & \text{if } b = 0 \\ cb_1, cb_2, \dots, -cb_\alpha, -cb_\beta, \dots, cb_n, & \text{if } b \neq 0 \text{ and } \alpha \oplus \beta = b \end{cases} \quad (9)$$

3.2.3. Embedding Cipher into Digital Image using Proposed Technique

Image steganography is the art of hiding secret data into digital images as carrier, where the main aim should be to make the hidden data more secure against the effect of steganalysis by reducing the rate of distortion in the stego-image. Usually in images, the pixel values of nearby pixels will be closely related. But when some data is embedded into these images by changing the pixels values and if the difference between the changed pixel and the actual pixel is high, then it results in high distortion of stego image and hence it could be easily detected by steganalysis. Hence the pixels in which the secret message is to be embedded should be selected with more care, in order to prevent the stego-image from steganalysis and distortion.

To provide the ability of high level security in smart cards, this proposed work has been implemented in such a way that the data to be secured is initially processed with public key cryptography using ECC and then the encrypted cipher is embedded into the digital photographic image of user. Here, steganography is performed by using an optimized modified matrix encoding technique. This optimized data hiding technique is a unique mechanism combining modified matrix encoding technique and artificial bee colony algorithm. In this optimized data hiding technique, initially a cover block is selected and the secret message (i.e. cipher) in the message block is embedded into the cover block by changing its binary pixel values.

Let *I* be the digital photographic image of the user of size $M \times N$ and let *S* be the secret message. The matrix form of image *I* is given as,

$$I = \begin{bmatrix} I_{11} & I_{12} & \dots & \dots & I_{1N} \\ I_{21} & I_{22} & \dots & \dots & I_{2N} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ I_{M1} & I_{M2} & \dots & \dots & I_{MN} \end{bmatrix}$$

Then based on the size of the message block MB , the cover block CB in which the bits of MB are to be embedded is selected randomly using a sliding window. Let the size of MB be L and hence a CB of same size is selected.

$$CB = \sum_{i=1}^L cb_i \quad (10)$$

The cover block pixels can be selected by,

$$CB = \begin{bmatrix} cb_{\alpha} & cb_{\alpha+1} & cb_{\alpha+n} \\ cb_{\alpha+N} & cb_{\alpha+(N+1)} & cb_{\alpha+(N+n)} \\ cb_{\alpha+2N} & cb_{\alpha+(2N+1)} & cb_{\alpha+(2N+n)} \end{bmatrix} \quad (11)$$

where α is any initial random pixel value and the remaining pixel values of the cover block are based on this representation. When CB has been selected, the cipher is embedded into it based on XOR functionality of matrix encoding. The modified image pixel M_{cb} after embedding the secret message either by changing the pixel value or without making any change could be derived from,

$$M_{cb_i} = \sum_{i=1}^n \{((mb_i \oplus cb_i) \cdot \overline{cb_i}) + (\overline{(mb_i \oplus cb_i) \cdot cb_i})\} \quad (12)$$

where mb and cb are the message block bits and the cover block bits respectively.

Now the modified cover blocks are obtained and if the secret messages were embedded into cover block by changing their values, then this results in distortion of the cover block pixel values. Hence it is necessary to find the amount of change between the actual cover block pixel values and the modified pixel values. This distance is calculated using the following equation.

$$d = \sqrt{\sum_{j=1}^n (cb_j - mb_j)^2} \quad (13)$$

Similarly, the distortion level in each modified cover block is calculated and the overall average distance is set as the fitness value. Then using ABC evolutionary optimization algorithm, a new set of cover blocks is selected and the secret messages are embedded and its overall fitness is evaluated. This

process continues until the fitness, i.e, the distance between the original cover block and modified cover block becomes very low. Finally when the optimal blocks for embedding secret message are found, the index values of those blocks are embedded either at the initial or final pixels of the image.

3.3. Image and Information recovery

At the receiver side, the following steps are performed to recover the secret message.

- ❖ Divide the stego-image I_M into M number of blocks, which is denoted as I_w^M , and extract the initial pixel value which contains the index values of the modified cover blocks.
- ❖ Perform vertical raster scanning process on the image I_w^M based on the index values.
- ❖ Select the modified cover blocks by index based on eq.11.
- ❖ Extract the pixels from the selected cover blocks and compute their binary values and then the ASCII values to retrieve the encrypted cipher.
- ❖ Decrypt the cipher to obtain the original message by using public key, and allow access if the user is authenticated.

4. RESULTS AND DISCUSSION

The proposed secure technique using ECC and an Optimized Modified Matrix Encoding technique is implemented in the working platform of MATLAB version 7.12. The given input information is encrypted by ECC and the secret message is embedded in the input image. The sample image used for this implementation is shown in figure 2.



Figure 2: Sample Input Cover Image

The encrypted cipher message is embedded into the sample input cover image and we obtain the message embedded stego-image, which is shown in Figure. 3.





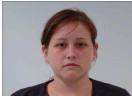





Steganography Image



Figure 3: Stego-Image







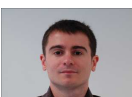



The performance of this proposed method is analyzed by embedding the secret message into five images and their PSNR values and Distance values (fitness) are demonstrated in Table 1.

Table 1: Performance Results Of Proposed Technique

Message	Cover Images	Stego-Images	Retrieved Image PSNR value	Maximum Distance values	Minimum Distance values	Extracted Message
HELLO			45.8603	60.4318	47.0319	HELLO
			40.2438	60.6877	51.1566	HELLO
			41.6862	60.0417	54.754	HELLO
			36.3978	66.453	55.6507	HELLO
			41.6944	61.4898	40.6448	HELLO

This proposed methodology is compared with the performance of Least Significant Bit (LSB) steganography. The result of the existing LSB technique is demonstrated in Table 2. As can be seen from table 1 and 2, our proposed technique performance is high in terms of PSNR value and distance values than the conventional technique, which means that the proposed technique reduces distortion in stego-image.

Table 2: Performance Results Of Existing Technique

Message	Cover Images	Stego-Images	Retrieved Image PSNR value	Maximum Distance values	Minimum Distance values	Extracted Message
HELLO			25.0452	169.1449	169.0739	HELLO
			25.1568	169.136	169.0739	HELLO
			25.4688	169.1538	169.0621	HELLO
			25.1888	169.1213	169.0710	HELLO
			27.3910	169.1153	169.0592	HELLO

By comparing the results of our proposed technique and the existing conventional technique, it is undoubtedly very clear that proposed technique's performance is comparatively higher than existing technique. The results exhibit the maximum distance values and minimum distance values between the original image and the stego-image. The proposed optimized embedding technique has reduced the distance between the original image and stego image from 60.4318 to 47.0319 for the first image, 60.6877 to 51.1566 in second images and so on, whereas the conventional techniques distance values are very high and it has also failed to optimize the distance values. Similarly, the PSNR value of the conventional technique is also very low compared to the proposed secure technique.

5. CONCLUSION

Higher level of authentication is required for the security of usage of password in many of the transactions. Even though, there are biometric authentications to restrict the unauthorized users, a more trusted system was needed to make the security appropriate for logical access. In this paper, we have implemented a secure technique by integrating a cryptographic technique and a steganographic technique. By making use of ECC for encrypting the user data, this technique has used

the most secured cryptographic algorithm. The main advantage of using ECC is its small key size. Also for embedding the cipher optimized modified matrix encoding technique has been used and this embeds more number of secret bits and at the same time reduces the distortion in the stego-image. From the results of this implementation, it is clear to conclude that this proposed secure technique has overcome the conventional technique in terms of PSNR values and Distance values. Also this technique has optimized the distance values to a pretty great extent. Hence this technique can be used for the purpose of security in conventional cryptographic smart cards where security is under great threat.

REFERENCES

- [1] Simon Liu and Mark Silverman, "A practical guide to biometric security technology", *IT Professional*, Vol. 3, No. 1, pp. 27- 32, 2001.
- [2] AdityaBodake, VirajBaviskar, AshwiniBodake, ShitalBhoite and N. J. Kulkarni, "Multipurpose Smartcard System", *International Journal of Advanced Research in Computer Engineering & Technology*, Vol. 1, No. 9, pp. 175-178, November 2012.



- [3] Katherine M. Shelfer and J. Drew Procaccino, "Smart card evolution", *Communications of the ACM - How the virtual inspires the real*, Vol. 45, No. 7, pp. 83-88, July 2002.
- [4] C.-B. Breunese, N. Cataño, M. Huisman and B. Jacobs "Formal methods for smart cards: an experience report", *Science of Computer Programming*, Vol. 55, No. 1-3, pp. 53-80, March 2005.
- [5] Hoon Ko and Ronnie D. Caytiles, "A Review of Smartcard Security Issues", *Journal of Security Engineering*, Vol. 8, No. 3, 2011.
- [6] Naccache, D and M'Raihi, D, "Cryptographic smart cards", *Micro, IEEE*, Vol. 16, No. 3, pp. 14, 16 - 24, Jun 1996.
- [7] Damien Sauveron, "Multiapplication smart card: Towards an open smart card?", *Information Security Technical Report*, Vol. 14, No. 2, pp. 70-78, May 2009.
- [8] Adi Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies", *Cryptographic Hardware and Embedded Systems*, Vol. 1965, pp. 71-77, 2000.
- [9] M. Abadi and M. Burrows, "Authentication and delegation with smart-cards", *Science of Computer Programming*, Vol. 21, No. 2, 93-113, October 1993.
- [10] C.-C. Chang and S.-J. Hwang, "Using smart cards to authenticate remote passwords", *Computers & Mathematics with Applications*, Vol. 26, No. 7, 19-27, October 1993.
- [11] Tao Xiang, Kwok-wo Wong and Xiaofeng Liao "Cryptanalysis of a password authentication scheme over insecure networks", *Journal of Computer and System Sciences*, Vol. 74, No. 5, pp. 657-661, August 2008.
- [12] Gabriele Lenzini, Mortaz S. Bargh and Bob Hulsebosch, "Trust-enhanced Security in Location-based Adaptive Authentication", *Electronic Notes in Theoretical Computer Science*, Vol. 197, No. 2, pp. 105-119, 22 February 2008.
- [13] Horng-Twu Liaw, Jiann-Fu Lin and Wei-Chen Wu, "An efficient and complete remote user authentication scheme using smart cards", *Mathematical and Computer Modelling*, Vol. 44, No. 1-2, pp. 223-228, July 2006.
- [14] Andrew Teoh Beng Jin, David Ngo Chek Ling and Alwyn Goh, "Biobhashing: two factor authentication featuring fingerprint data and tokenized random number", *Pattern Recognition*, Vol. 37, No. 11, pp. 2245-2255, November 2004.
- [15] Qi Xie, "Improvement of a security enhanced one-time two-factor authentication and key agreement scheme", *Scientia Iranica D*, Vol. 19, No. 6, pp. 1856-1860, 2012.
- [16] Guomin Yang, Duncan S. Wong, Huaxiong Wang and Xiaotie Deng, "Two-factor mutual authentication based on smart cards and passwords", *Journal of Computer and System Sciences*, Vol. 74, pp. 1160-1172, 2008.
- [17] I-En Liao, Cheng-Chi Lee and Min-Shiang Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, Vol. 72, PP. 727-740, 2006.
- [18] Rajaram Ramasamy and Amutha Prabakar Muniyandi, "An Efficient Password Authentication Scheme for Smart Card," *International Journal of Network Security*, Vol. 14, No. 3, PP. 180-186, May 2012.
- [19] Yadollah Eslami, Ali Sheikholeslami, P. Glenn Gulak, Shoichi Masui, and Kenji Mukaida, "An Area-Efficient Universal Cryptography Processor for Smart Cards," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 14, No. 1, January 2006.
- [20] Sandeep Kumar Sood, "An Improved and Secure Smart Card Based Dynamic Identity Authentication Protocol," *International Journal of Network Security*, Vol. 14, No. 1, PP. 39-46, Jan. 2012.
- [21] Manoj Kumar, "An Enhanced Remote User Authentication Scheme with Smart Card," *International Journal of Network Security*, Vol. 10, No. 3, PP. 175-184, May 2010.
- [22] YongSoo Choi and Hyounghoong Kim, "Improving the modified matrix encoding on steganography method", *In Proceedings of the fifth International Conference on Information Assurance and Security*, China, August 18-20, 2009.
- [23] S. Brindha and Ila. Vennila, "Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart Card based Authentication System", *International Journal of Computer Applications*, Vol. 26, No. 10, July 2011.
- [24] Olaniyi. O. M, Arulogun . O. T. and Omidiora E.O, "Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting", *African Journal of Computing & ICT*, Vol. 5, No. 6, December 2012.



- [25] H S Manjunatha Reddy and K B Raja, "Wavelet based Non LSB Steganography", *International Journal of Advanced Networking and Applications*, Vol. 3, Issue. 03, Pages. 1203-1209, 2011.
- [26] Andreas Westfeld, "F5- A Steganographic Algorithm High Capacity Despite Better Steganalysis", *In Proceedings of 4th International Workshop on Information Hiding, Pittsburg, USA*, pp. 289-302, 2001.