ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 3, March 2017

Secure Information Sharing Using Image Cryptography

K.R.Deepa[1], V.Kiruthiga[2], S.Nandhini[3], S.Narmatha[4]

Assistant Professor, Dept. of ECE, V.S.B Engineering College, Karur, Tamilnadu, India[1]

UG Student, Dept. of ECE, V.S.B Engineering College, Karur, Tamilnadu, India[2,3,4]

ABSTRACT: In this paper we purposed an image based cryptography that Elliptic Curve cryptography (ECC) techniques and encoding technique on images to enhance the security of the communication Channel. In the ECC approach, the basic idea is to replace the Elliptic Curve cryptography (ECC) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The ECF-based technique is the most challenging one as it is difficult to differentiate between the cover-object and Crypto- object if few ECC bits of the cover object are replaced. Millions of images are transferred everyday across the network. Some of these images are confidential and we want these images to be transferred securely. Cryptography plays a significant role in transferring images securely. The exponentially hard problem to solve an Elliptic Curve Discrete Logarithm Problem with respect to key size of Elliptic Curve Cryptography helps in providing a high level of security with smaller key size compared to other cryptographic technique which depends on integer factorization or Discrete Logarithmic problem. In this paper, we implement the Elliptic Curve cryptography to encrypt, decrypt and digitally sign the cipher image to provide authenticity and integrity.

KEYWORDS: Cryptography, Elliptic Curve cryptography (ECC), Discrete Logarithm.

I.INTRODUCTION

The word cryptography is derived from the Greek words Crypto meaning cover and grafia meaning writing defining it as covered writing. In image cryptography the information is hidden exclusively in images. Cryptography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as Crypto-medium. A Crypto-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. A lot of information is perceived when we observe an image. Images have become an inevitable source of information. Every day we come across various image from various sources. When images are confidential and we want the image to be transferred safe and securely, cryptography comes into play. The cryptographic technique which we have implemented in this paper is the Elliptic Curve Cryptography (ECC). Various study on ECC has concluded that the difficultly to solve an Elliptic Curve Discrete Logarithmic Problem is exponentially hard with respect to the key size used. This property makes ECC a very good choice for encryption/decryption process compared to other cryptographic techniques which are linearly difficult or sub exponentially difficult.

II.RELATED WORK

The space of difference password is very small. For example, there are limited places available to select to cook a meal. In the case of hiding object in a room, the requirements to hide objects already strongly reduce the state space. It would be better if the user could place object in arbitrary locations. There are only a few places in the given room where the object can be really hidden for example under the mattress or the cabinet are location which users are likely to select. Furthermore, the system allows users to picks the password. For example, choosing all the aces in the deck of cards in certainly not secure. It is likely that many users will commonly know n combinations, for example by choosing to mix the same drinks. Finally, the system required user to precisely recall the authentication task, instead of relying on recognition. Another weakness is that an attacker will only need to break the v- password to get access to all the users

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 3, March 2017

other password. In this paper plain text is converted into cipher text because third parties cannot hack the data. Here, the data can be hide inside of the image. The user only knows the key value so the data will be secured.

III. PROPOSED FORGERY DETECTION METHODOLOGY

To decrease the number of computational steps in ECC operation, we perform two operations defined below.

Pixel grouping into a single integer

Images are made up of pixels. If cryptographic operation is performed on every single pixel it will take more time as the number of pixels present is very large. So, it will be a good option to group the pixels together. The number of pixels to be group depends on the Elliptic Curve parameters used. The larger the parameter of the elliptic curve, the more pixel can be grouped. For example a 512 bit ECC parameter can group up to 63 pixels together. To get the number of pixels to be group, find the number of the list, of the base 256 digits in the integer ' p' minus 1. To convert the group of pixels into a big single integer we have used a function of Mathematic called From Digits [list of pixels, b] which take a list of pixels and convert it to base b. We add random 1 or 2 to each pixel to avoid error caused while using From Digits function of Mathematic, in case, the first pixel value of the group is 0 and also to provide low correlated pixel value for the cipher image generated with same pixel value plain image. Pixel value of image in byte form will range from 0 to 255. So the maximum possible pixel value of the image will be 257 including the 2 we added. So, we will use base value 'b' as 258.

Getting the group of pixels from the big integer

After the ECC operation the coordinate value will all be in the range of the bit size chosen for the ECC operation. To generate the cipher image from these coordinates we need to bring it down to 0 to 255 range. We performed using the Integer Digits [big integer value, 256] function in Mathematical. It takes as input the big integer values in the range of the size chosen for ECC operation and with base 256, the output will be a list of values ranging from 0 to 255. The two function, From Digits[ ] and Integer Digits[ ] are inverse of each other so the pixels value are preserved during the operation. Mathematical o operation on an image is done on the pixels value of the image. So first, we get the pixels value of the image. The Elliptic curve parameters {a, b, G, p} are agreed between the sender and the receiver. The sender use the public key 'Pb' of the receiver to generate the cipher image from the pixels of the plain image. The receiver use the private key 'nB' which was used to generate the public key, to decrypt the cipher image back to the plain image.

Image encryption

1. Get the pixel value of the image to be encrypted and randomly add 1 or 2 to each pixel. Record the number of channels present in the image.
2. Group the pixels and convert to single large integer value for each group. Number of pixel to be group using Mathematical is given by gr p = Length [Integer Digits[p, 258]] − 1
3. Pair up the result obtained from step 2 and store as 'Pm' which is the plain message input for the ECC system.
4. Select a random 'k' and compute 'kG' and 'kPb' where 'Pb' is the public key of the receiver.
5. Perform point addition of 'kPb' with each value of 'Pm' and store as 'Pc' which is the cipher text.
6. Convert the cipher text list from step 5 to value ranging from 0 to 255.
7. Pad left with 0 to each list from step 6 which have less than gr p + 1 number of elements, to make each list equal in length.
8. Flatten the list from step 7, group them according to the number of image channels that we have recorded and partition them to width of the plain image.
9. Convert the values from step 8 into cipher image.

Digital signature on cipher image

For performing digital signature we can still use the ECC parameters used for encryption.

1. The sender selects a private key 'n A' and generate the public key Pa = nAG.
2. Get the Hash value of the pixel values of the cipher image and store as 'z'.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 3, March 2017

3. Sender select a random integer 'k' in the range of [1 to n − 1] where n is the cyclic order of the Elliptic Curve with G as Generator.

4. Compute the digital signature pair {r,s} where r = {kG} mod [n]x−coordinate (11) s = z + rnA k mod [n] (12) Send kG, cipher image, Digital Signature {r,s}.

Image Decryption

1. Get the pixel value of the cipher image and group by gr p + 1 number of pixels and form single big integer value for each group with base 256. Record the number of image channels of the cipher image.
2. Pair up the value obtained from step 1.
3. Perform point multiplication of 'kG' with 'nB' where 'nB' is the private key of the receiver.
4. Perform point subtraction between values from step 2 with value from step 3.
5. Get the value in the range of 0 to 255 from step 4 with base 258 and subtract random 2 from each value.
6. Group the flatten value obtained in step 5 in term of recorded number of image channels of the cipher image and partition them to the width of the cipher image.
7. Convert the values from step 6 into plain image.

Verifying the signature

1. Calculate hash value of cipher image pixel value.
2. Obtain w = 1 s mod [n] (13)
3. Calculate u1 = {z ∗ w} mod [n] (14) u2 = {r ∗ w} mod [n] (15)
4. Compute {x1, y2} = u1G + u2Pa (16)
5. If r == {x1} mod [n] (17) signature is verified.

IV. ALGORITHM BASED METHODS

Elliptic curve cryptography (**ECC**) is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra_elliptic curve factorization. **Elliptic curve cryptography** (ECC) is an approach to public-key **cryptography** based on the algebraic structure of **elliptic curves** over finite fields. ... They are also **used** in several integer factorization algorithms that have applications in **cryptography**, such as Lenstra **elliptic curve** factorization.. In mathematics, an **elliptic curve** is a plane algebraic **curve** defined by an equation of the form. that is non-singular; that is, its graph has no cusps or self-intersections. Elliptic curve cryptography (ECC) can provide the same level and type of security as RSA (or Diffie-Hellman as used in the manner described in Sect with much shorter keys. As you saw in Section 12.12 of Lecture , the computational overhead of the RSA-based approach to public-key cryptography increases with the size of the keys. As algorithms for integer factorization have become more and more efficient, the RSA based methods have had to resort to longer and longer keys. Elliptic curve cryptography (ECC) can provide the same level and type of security as RSA (or Diffie-Hellman as used in the manner described in Section 13.5 of Lecture 13) but with much shorter keys. Compares the key sizes for three different approaches to encryption for comparable levels of security against brute-force attacks. What makes this table all the more significant is that for comparable key lengths the computational burdens of RSA and ECC are comparable. What that implies is that, with ECC, it takes one-sixth the computational effort to provide the same level of cryptographic security that you get with 1024-bit RSA. The computational overhead of both RSA and ECC grows as O(N3) where N is the key length in bits. [Source: Hank van Tilborg, NAW, 2001] Nonetheless, despite this parity in the dependence of the computational effort on key size, it takes far less computational overhead to use ECC on account of the fact that you can get away with much shorter keys. Because of the much smaller key sizes involved, ECC algorithms can be implemented on smartcards without mathematical coprocessors.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 3, March 2017

V. EXPERIMENTS AND RESULTS

We have implemented the above two techniques in MATLAB and the above mentioned algorithms with respect to image cryptography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the cryptographic system. Some parameters are as follows Perceptibility does embedding information distort cover medium to a visually unacceptable level. Capacity how much information can be hidden (relative to the change in perceptibility) item. Robustness to attacks can embedded data survive manipulation of the Crypto medium in an effort to destroy, remove, or change the embedded data.

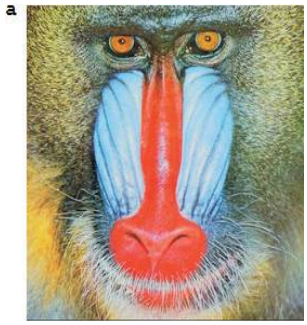

Fig.1 Plain image of mandrill

STEP 1: Take any original image .

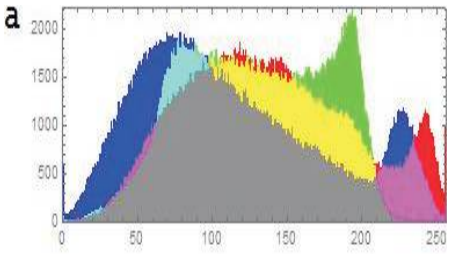

Fig. 2 Histogram of mandrill

STEP 2: Original image is convert into histogram value.

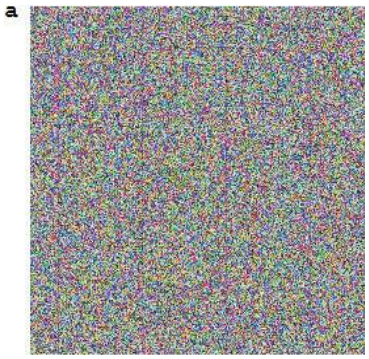

Fig. 3 Cipher image of mandrill

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 3, March 2017

STEP 3: Original image is convert into cipher image form.

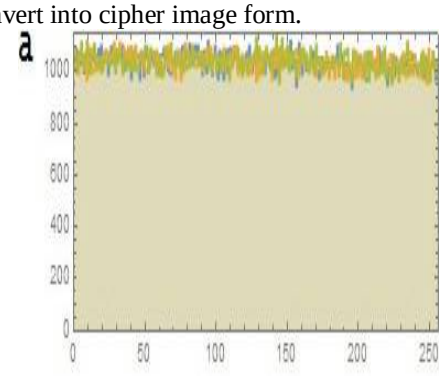

Fig. 4 Histogram of cipher mandrill

STEP 4: Cipher image is converted into histogram value.

Cipher Image	Size	Entropy
Mandrill	256*260	7.99884

Fig.5 Table value for mandrill size and entropy

STEP 5: Cipher image size and entropy of mandrill.

VI. CONCLUSION

In the paper we have presented the implementation technique of image encryption/decryption and inclusion of digital signature to the cipher image to provide authenticity and integrity to the received image. We have performed our operation by grouping the pixel and explained how many pixels can be grouped according to the ECC parameters. Pairing of the grouped pixel value was performed instead of mapping those values to Elliptic curve coordinate. It helps to ignore the used of reference mapping table for encryption and decryption. Our algorithm generates a low correlated cipher image even with a image which is made up of same pixel value. We have also analysed our technique to support the strength of the algorithm.

REFERENCES

[1] Lawrence C. Washington, ***"Elliptic Curves Number Theory and Cryptography"***, Taylor & Francis Group, Second Edition, (2008).
[2] A. Ahmed, Abd El-Latif and Xiamu Niu, ***"A Hybrid Chaotic System and Cyclic Elliptic Curve for Image Encryption"***, In AEU-International Journal of Electronics and Communications, Elsevier, issue 2, vol. 67, pp. 136–143, (2013).
[3] Hong Liu and Yanbing Liu, ***"Cryptanalyzing an Image Encryption Scheme based on Hybrid Chaotic System and Cyclic Elliptic Curve"***, In Optics and Laser Technology, Elsevier, vol. 56, pp. 15–19, (2014).
[4] S. Maria Celestin Vigila and K. Muneeswaran, ***"Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications"***, In International Journal of Network Security, vol. 14, no. 4, pp. 236–242, July (2012).
[5] Ali Soleymani, Md Jan Nordin and Zulkarnain Md Ali, ***"A Novel Public Key Encryption based on Elliptic Curves Over Prime Group Field"***, In Journal of Image and Graphics, vol. 1, pp. 43–49, (2013).
[6] S. Behnia, A. Akhavan, A. Akhshani and A. Samsudin, ***"Image Encryption based on the Jacobian Elliptic Maps"***, In The Journal of System and Software, Elsevier, vol. 86, pp. 2429–2438, (2013).
[7] Li Li, Ahmed A. Abd El-Latif and Xiamu Niu, ***"Elliptic Curve ElGamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images"***, In Signal Processing, Elsevier, vol. 92, pp. 1069–1078, (2012).
[8] Don Johnson, Alfred Menezes and Scott Vanstone, ***"The Elliptic Curve Digital Signature Algorithm (ECDSA)"*** , Certicom Corporation, (2001).
[9] Lo'ai Tawalbeh, Moad Mowafi and Walid Aljoby, ***"Use of Elliptic Curve Cryptography for Multimedia Encryption"***, IET Information Security, vol. 7, issue 2, pp. 67–74, (2012).
[10] Ann Hibner Koblitz, Neal Koblitz and Alfred Menezes, ***"Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift"***, In Journal of Number Theory, Elsevier, vol. 131, pp. 781–814, (2011).