IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-8 E-ISSN: 2347-2693

Design and Evaluation of Performance for Text and Image Cryptography Using Biometric Key and ECC

Anu Kukreja[1*] and Ayushi [2]

[1*,2]Department of Computer Science and engineering, HCE Sonepat

www.ijcaonline.org

Received: 18/07/ 2014 Revised: 30/07/ 2014 Accepted: 22 /08/ 2014 Published: 31 /08/ 2014

Abstract - Cryptography is one of the important sciences in the current era. It is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text .Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. The importance of cryptography comes from the intensive digital transactions which we daily perform on the internet and other communication channels. Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. A visual cryptography scheme encodes a black and white secret image into *n* shadow images called shares which are distributed to the *n* participants. Such shares are such that only qualified subsets of participants can "visually'' recover the secret image. Elliptical curves are mathematical NP-hard problems, which are proofed to be intractable in term of complexity. Cryptography has efficiently utilized the strength EC in developing several cryptosystems such as key agreement protocols, digital signatures and others. Elliptic Curve Cryptography (ECC) usage is with smaller key to give high security and high speed in a low bandwidth. ECC is considered as the best method for upcoming applications. There are number of existing cryptographic approaches. In this present work, we have defined a hybrid cryptography approach with the combination of biometric key concept and the Elliptical Curve Cryptography (ECC). ECC is a public key cryptography having equal and attractive significance over RSA algorithm with smaller key size. It is based on geometric elliptical curve design algorithm. In this work, the authentication of the user will be verified based on the user information as well as the signature. It means the cryptography will be performed over the text information as well as on digital signature. This two layer scheme will improve the security for the authentication. The proposed algorithm is implemented on both text and image for encoding and decoding purpose. All the implementation work has been done in MATLAB R2009 using general MATLAB toolbox and image processing toolbox. Encryption time, decryption time and size of encrypted data have been taken as parameter for evaluation of performance of algorithm.

Keywords- Elliptic Curve Cryptography (ECC), cryptography, biometric image, text, encryption, decryption.

1. INTRODUCTION

Cryptography is the study of Secret (crypto-)-Writing (-graphy).It is the art or science of principles and methods of transforming an understandable message into one that is not understandable and then transforming the message back to its original form. In today's life Cryptography is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under complicated situations. Authentication is as essentially a part of our lives as confidentiality. The Author use authentication throughout our everyday lives when we sign our name to some document and for instance and , as we move to world where our decisions and agreements are communicated electronically via e-mail or any other means, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures. A digital signature another cryptographic technique, binds a document to the owner of a particular key, while a digital time stamp (another cryptographic technique) binds a document to its creation of a particular time [1]. These cryptographic mechanisms can be used to control access to shared disk drive, a high security installation, or a pay-per-view TV channel etc. The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build complex schemes and protocols that allow us to pay using electronic money, to prove we know certain information without revealing the information itself, and to share quantity in such a way that a subset of the shares can reconstruct the set. While modern cryptography is growing increasingly, cryptography is fundamentally based on problems that are difficult to solve [2][3]. A problem may be difficult because its solution requires some secret knowledge such as decrypting an encrypted message or signing some digital document.

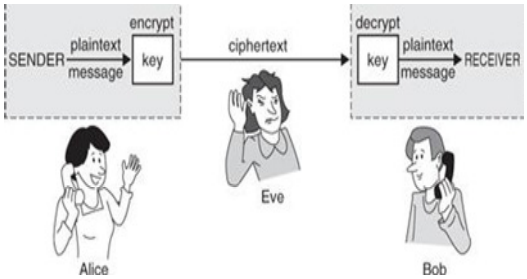

Fig. 2.1 Process of Cryptography [7]

Corresponding Author: *Anu Kukreja*

Fig. 2.1 shows the process of Cryptography which is the science of secret sharing. Any character or alphabet we press on the keyboard is represented as binary information. If the entire document is converted into binary information, just imagine how difficult it would be to recognize the information. In the process of encryption, we try to mix these binary numbers after performing a few mathematical operations which converts the huge set of binary information in a newer arrangement which is difficult to understand.

II. ELLIPTIC CURVE CRYPTOGRAPHY

Public key cryptography systems are usually based on the assumption that a particular mathematical operation is easy to do, but difficult to undo unless you know some particular secret. A recent development in this field is the so-called Elliptic Curve Cryptography. Elliptic Curve Cryptography works with point on a curve. The security of this type of public key cryptography depends on the elliptic curve discrete logarithm problem. Elliptic curve cryptography was invented by Neil Koblitz in 1987 and by Victor Miller in 1986. The principles of elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or EIGamal. Although no general patent on elliptic curve cryptography appears to exist, there are several patents that may be relevant depending on the implementation [4]. The main advantage of elliptic curve cryptography is that the keys can be much smaller. Recommended key sizes are in the order of 160 bits rather than 1024 bits for RSA [8].

A. Elliptic Curves

An elliptic curve is a set of points (x, y), for which it is true that

$$y2 = x3 + ax + b$$

Given certain chosen numbers a and b. Typically, the numbers are integers (whole numbers), although in principle the system also works with real (fractional) numbers. Despite what the name suggests, the curves do not have an elliptic shape. For example, -4 and b = 0.67 gives the elliptic curve with equation y2= x3 - 4x + 0.67. This curve is illustrated in Figure 2.2

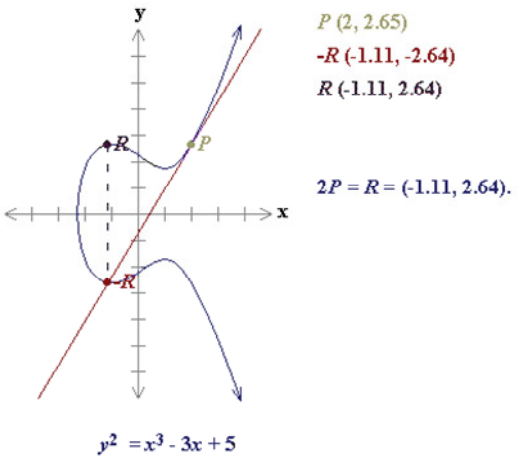

Fig. 2.2 The geometry of point doubling on Elliptic Curve [6]

If x3 + ax + b contains no repeated factors, or equivalently if 4a3 + 27b2 is not 0, then the elliptic curve can be used to form a group. A group is simply a set of points on the curve. Because it is a group, it is possible to "add up" points which give another point on the curve. On the graph, two points are added up by drawing a line through both and taking as the outcome where the line intersects the curve. For cryptographic purposes, an elliptic curve must have only points with all coordinates whole numbers (integers) in the group. The trick with elliptic curve cryptography is that if you have a point F on the curve, all multiples of these points are also on the curve [4, 5].

B. Generating an Elliptic Curve Public key

Alice and Bob agree on an elliptic curve and pick a certain point F on this curve. They can do this with Eve listening in. Alice next picks a random number As (which does not have to be a point on the curve) and computes AI' = As*F. The point AI' is on the curve, [because it is a multiple of F. This is easy to compute Alice's public key is AI' and her secret key is As. Bob does the same thing and ends up with Bp and Bs [4].

C. Encrypting and Decrypting Messages

Alice and Bob can now secretly agree on a key with which they can encrypt messages sing secret key cryptography. The key simply is the product of Alice's public key and Bob's secret key (which is the same as the product of Alice's secret key and Bob's public key). It will be clear that Alice and Bob can compute this product after they have exchanged their public keys, but Eve cannot since she has none of the secret keys [4].

D. Cracking the Elliptic Curve Key

If Eve wanted to crack the key, she would have to reconstruct one of the secret keys. This means having to compute As given AI' and F (because AI' = As * F). And that is very difficult. The number of discrete points on the curve (points with both X and Y coordinates being integers) is called the order of the curve. If the order of the point F is a prime number of n bits, then computing As from As*F and F takes roughly 2"'2 operations. If F is, say, 160 bits long, then Eve needs about 280 operations. If she can do a billion operations per Second, this takes about 38 million years. This problem is commonly referred to as the elliptic curve discrete logarithm problem [4].

E. The Public Key cryptography (PKC)

Concept was first pioneered by Diffie and Hellman in 1976, in their influential article, New Directions in Cryptography. This article also tackled the key exchange issue, founded on the intractability of the discrete logarithm problem. In a public key cryptography, each party has a pair of keys, one distributed in public, known as the public key, and the other is saved in a secure place, known as a private key (secret key). Public key cryptography depends on the trapdoor function, that makes decryption achievable provided the knowledge of the secret key corresponding to the public key. Bearing in mind a case like the one explained within the symmetric keys case, whereby Alice needs to send a

message m to Bob. The following steps will achieve the task:

1) Alice passes Bob's public key B4 and the message m to a suitable encryption algorithm to form the encoded message.

$$C(\Sigma a(j)) = E(\Sigma a(j))$$

2) The encrypted message was sent by Alice to Bob.

3) Bob decrypts the encoded message received by him, via his private key Δ_B [5] and the suitable decryption algorithm [6].

Bob ensures that the data he received is not tampered with or leaked, as only his private key can decrypt the data. Likewise, Bob can transmit data to Alice using her public key A. The PKC scheme also fulfils the Non Repudiation and Authenticity by utilizing inventive approaches such as Digital Signatures. The PKC system is shown in Fig. 2.3.

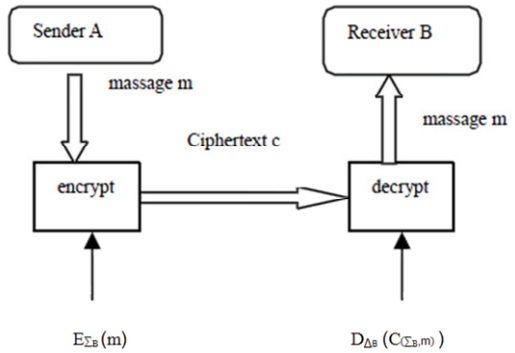

Fig. 2.3 PKC encryption [6]

III. PROPOSED ALGORITHM

A. *Image Encoding*

- Get the Biometric Face Image as input.
- Apply Gray Scale Thresholding over Image to perform Image Segmentation.
- Apply Watershed Algorithm to Extract the Key Features from Biometric Image.
- Apply the Edge Detection on watershed image to extract the effective key area.
- Apply the morphological operators to obtain the Biometric key for cryptography.
- Combine the Biometric Image with this extracted Key to perform key based cryptography.
- Obtain the Angular Analysis over image to generate rotation vector over image pixels.
- Perform rotational Transform over the image.
- Convert the Image to Signal Form.
- Obtain the key point respective to which cryptography is performed.
- Obtain the transform cryptography image after block wise transformation.
- Generate the Random Sequence to perform complex Cryptography.
- Apply Sequence Transformation over the image.
- Return Crypto Image

B. *Image Decoding*

- Inputting of encrypted image.
- Apply translation on encrypted image vector.
- Obtain size of image.
- Read the image row and column wise.
- Identify the block centre under the angular variation.
- Perform the rotation over image pixels.
- Generate the encrypted mil-line transformed image.
- Obtain the high intensity image area.
- Obtain the decoded biometric image.

C. *Text Encoding*

- Get the text as input.
- Estimate the Maximum number of possible characters in Info.
- Estimate the range of Bit symbols.
- Divide the frequency range in four quarters.
- Process all Data Bits.
- Get the character value.
- Convert the character to index form.
- Estimate the frequency of the character respective to occurrence.
- Encode the character based on frequency analysis and segmented blocks.
- Generate the Encoded String.
- Return Encoded Text.

D. *Text Decoding*

- Estimate the Maximum number of possible characters in Info.
- Estimate the range of Bit symbols.
- Divide the frequency range in four quarters.
- Process all Data Bits.
- Get the Encoded Character.
- Apply Decoding based on Frequency Analysis.
- Perform character transformation.
- Combine the character values.
- Return input text.

IV. EXPERIMENTAL RESULTS

We have defined and implemented a hybrid cryptography approach with the combination of biometric key concept and the Elliptical Curve Cryptography (ECC) using general MATLAB toolbox and image processing toolbox in MATLAB R2009. First, encoding of text and biometric image is done and then decoding of the same has been done. Figure 1 to 8 shows the full implementation from encoding to decoding. Figure 1 and 2 are the screenshots of biometric image and text to be encrypt. Figure 3 is the screenshot of biometric key generated so as to encrypt the image and text. Figure 4 and 5 are the screenshots of encrypted image and text. Figure 6 and 7 are the screenshots of decrypted image and text. After that, output parameter i.e. mean square error and PSNR has been calculated. Figure 8 is the screenshot of the same. Value of MSE is 5.2 and that of PSNR is 0.9. Also, text of cipher text and time for encryption and decryption is calculated. A comparison of computational time has also been made for basic ECC, improved ECC and

proposed algorithm. Figure 9 is the screenshot of the same. Figure 9 clearly shows that proposed algorithm is taking very much lesser time as compared to that of existing algorithm. Figure 10 is the screenshot of the plot of size of plane text and cipher text for ECC algorithm and figure 11 is the screenshot of the plot of size of plane text and cipher text for proposed algorithm. On comparing figure 10 and 11, it can be concluded that proposed algorithm produces a cipher text which consume lesser space as compare to that of ECC algorithm.

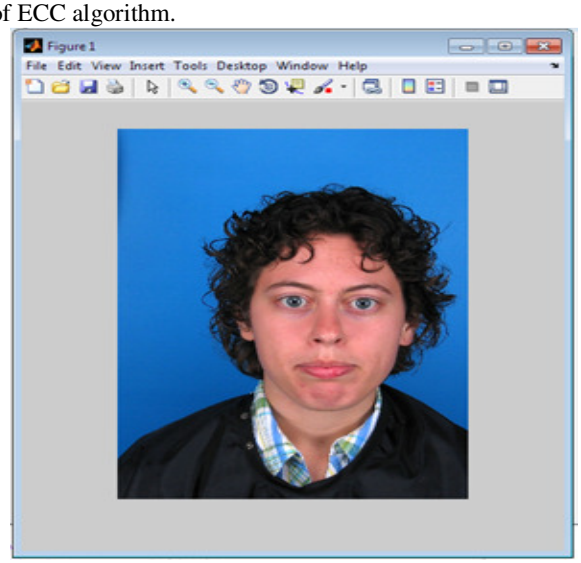

Fig. 4.1 Biometric image to be encrypt

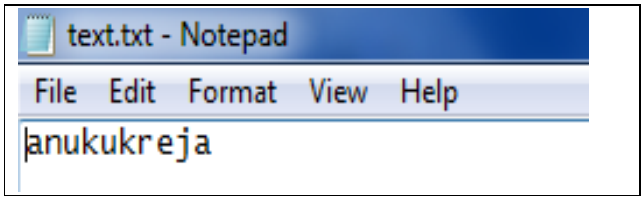

Fig. 4.2 Biometric text to be encrypt

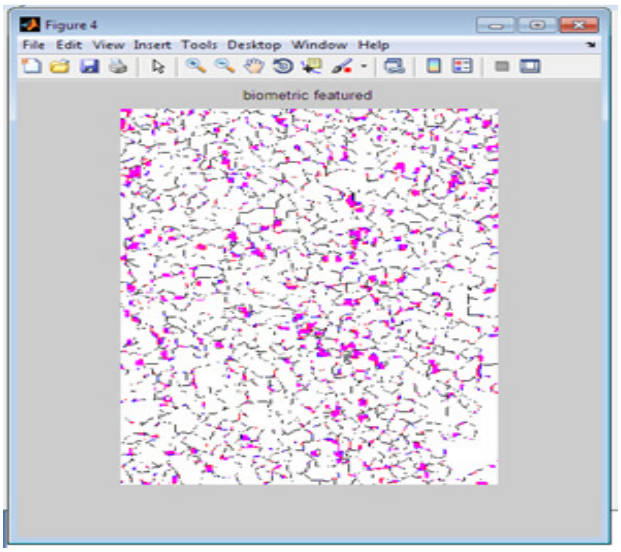

Fig. 4.3 Biometric key

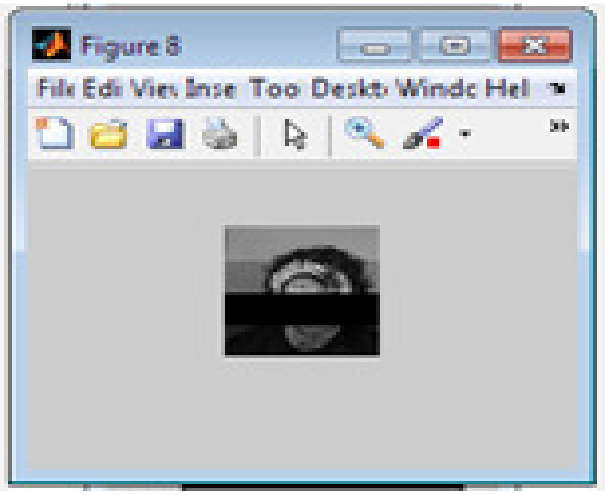

Fig. 4.4 Encrypted image

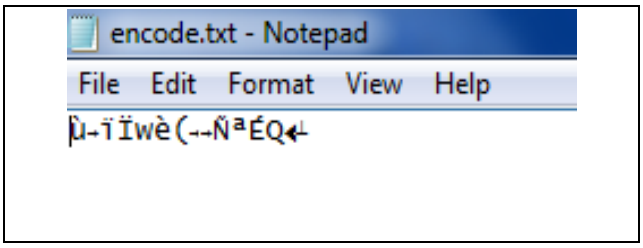

Fig. 4.5 Encrypted text

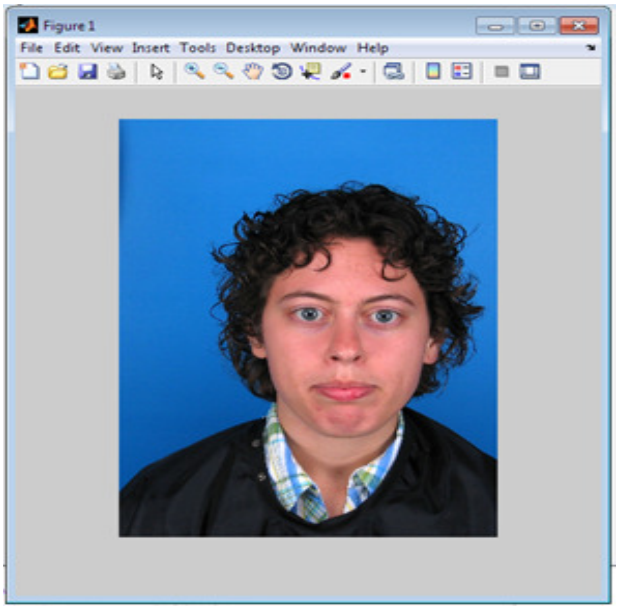

Fig. 4.6 Decrypted image

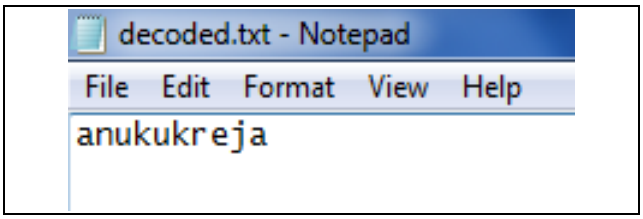

Fig. 4.7 Decrypted text

```
mse =

    5.212628681683318e+004

psnr =

    0.960235715325868
```

Fig. 4.8 screenshot of MSE and PSNR

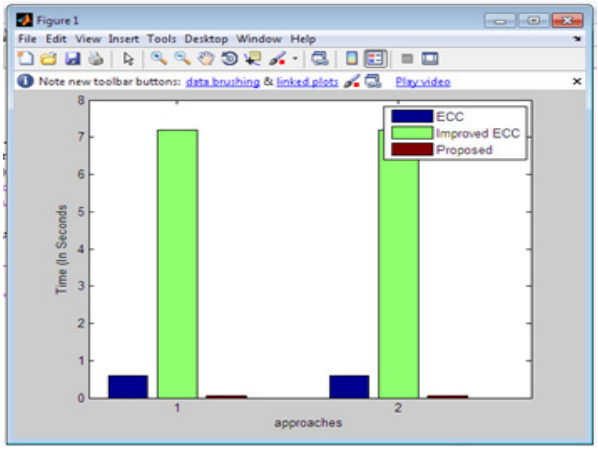

Fig. 4.9 Bar chart for computational time for Encryption and Decryption

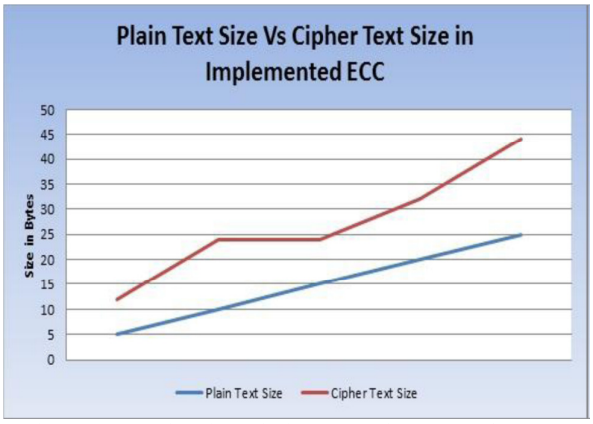

Fig. 4.10 plot for size of plane and cipher text for ECC algorithm [7]

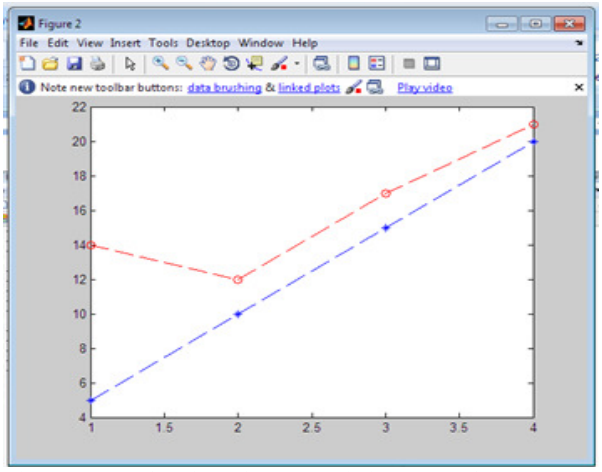

Fig. 4.11 plot for size of plane and cipher text for proposed algorithm

V. Conclusion And Future Scope

In this work, a hybrid cryptography algorithm has been proposed and examined. We introduced a framework to construct public-key cryptosystems using matrices over finite fields. This framework evolves from relating general systems of multivariate polynomial equations to the matrices. Using the general formula expressing this relationship, we designed a practical trapdoor one-way function. Existing literature on the subject of enhancing the performance of symmetric-key algorithms was discussed, followed by detailed descriptions of the targeted processor and the targeted cryptographic algorithms. Descriptions of the custom instructions were given along with the functional units that implement the underlying logical and arithmetic operations. Proposed method, while not a public-key system such as RSA, is almost unbreakable through brute force methods. It is susceptible to patterns, but this weakness can be avoided through first compressing the file (so as to remove patterns). This method requires that both encryptor and decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is nearly unbreakable. Both analysis and experiments on real multi-core prototypes show that proposed method provides a good speedup, large communication latency tolerance, good portability, and good scalability. These features make proposed method a good parallel-software solution for RSA, DSA, and ECC on multi-core systems. Future scope of this technique is big and can also be implemented in daily life use, but, the use of this technique in reality depends and varies from user to user. Also, Take high quality measures to pass more data in safe way making it not easy to detect the presence of messages or extract the messages from unwanted users. In the future work, the effectiveness of modified Variable Size Block encryption using dynamic Key Mechanism can be assessed under more complex information security environments.

REFERENCE

[1]. Farshid Delgosha, and Faramarz Fekri, "Public-Key Cryptography Using Paraunitary Matrices" IEEE transaction on signal processing, vil. 54, no. 9, September **2006**.

[2]. Sean O'Melia and Adam J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions" transaction on very large on very large scale integration system, Vol. 18, No. 11, November **2010**.

[3]. Zhimin Chen and Patrick Schaumont, "A Parallel Implementation of Montgomery Multiplication on Multicore Systems: Algorithm, Analysis, and Prototype" IEEE Transaction on computers, Vol. 60, No. 12, December **2011**.

[4]. Daniel Page and Frederik Vercauteren , "A Fault Attack on Pairing-Based Cryptography" IEEE Transaction on computers, Vol. 55, No. 9, September **2006**.

[5]. Zhi Zhou, Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography" IEEE Transaction on image processing, Vol. 15, No. 8, August **2006**.

[6]. Ohood S. Althobaiti1 and Hatim A. Aboalsamh, "An Enhanced Elliptic Curve Cryptography for Biometric".
[7]. Gururaja.H.S., M.Seetha, Anjan.K.Koundinya, "Design and Performance Analysis of Secure Elliptic Curve Cryptosystem" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August **2013**.
[8]. Vaibhav Choudhary, Kishore Kumar, Pravin Kumar and D.S. Singh, "Modified Pixel Sieve Method for Visual Cryptography" Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 321-326.

AUTHORS PROFILE

Anu kukreja is M.Tech Scholar in computer science department at Hindu College of engineering, sonepat, Haryana, india.

Ayushi is Assistant Professor in computer science department at Hindu College of engineering, sonepat, Haryana, india.

