# A Visual Cryptographic Technique for Transferring Secret Image in Public Cloud

**Ashok Kumar J, Gopinath Ganapathy**

***Abstract**: The use of "Asymmetric Cryptography" provides the way to avail the feature of non-repudiation, encryption of data and defining the user digital identity to map with the authenticating user in the Public Cloud. A security technique is to be provided for the data even before it is stored on the Cloud. The public key certificate can be transferred into key server for encrypting the data by other users or devices in the public cloud. By using OpenPGP standard (PGP)/GNU Privacy Guard (GnuPG), public key certificate and the private key certificate can be generated by the user in the client system itself. The client private key can never be moved out from the client system and users only responsibility is to decrypt their data like images. This methodology will be very much suitable for authenticating, transferring, accessing and storing the images in the Public Cloud. The computational cost for encrypting the whole image with public key will be huge and so the hybrid methodology is proposed with visual cryptography technique and Elliptic-Curve Diffie–Hellman (ECDH) methodology. This paper proposes secure transfer of secret image by using visual cryptography technique and thereby modifying any one of the visual shares into encrypted data with ECDH secret key and finally converted those two shares into base64 format. The proposed algorithm is implemented by using the Python language and their results are discussed with sample images.*

***Keywords** : Cloud Storage, Elliptic Curve Cryptography, ECDH, Visual Cryptography.*

## I. INTRODUCTION

In public cloud, image encryption is essential to transmit an image securely through insecure network prohibiting the unauthorised user to access, so that the decryption of an image is impossible by third party. Image encryption is utilized in several fields like Medical Image Processing, Telecommunication and Banking etc. The encryption solutions are taken more seriously for secure computations, secure service usage and secure storage in the public cloud.

All the users in the public cloud can store their bulk data and retrieve those data from the "Cloud Storage" based on the data access control policies defined by the cloud service provider [1]. But users are losing their control on their data and the security is the main question for accessing those data by other users in the cloud storage. So, security access control policy is to be correctly available in the hands of the user. Inorder to provide security for the sensitive data, the data confidentiality needs to be achieved before it is stored in the public cloud. In this paper, the hybrid methodology of Elliptic Curve Cryptography (ECC) and Visual Cryptography technique is proposed to protect the data on the fly and data at rest in the cloud storage. The computational cost for encrypting the whole image can be minimized with this hybrid approach of visual cryptography technique using ECC Algorithm.

## II. VISUAL CRYPTOGRAPHIC

Shamir and Naor proposed a new concept called visual cryptography used to encrypt images, texts, handwritten data and human intervention is needed for decryption. The brute force attack is not possible to ascertain the decoded image. Visual cryptography [2] deals with the secret sharing of data like images and does not reveal any share of the original image. For example, Alice sends the secret data to Bob and the secret data is converted into two shares, so that it will not reveal any share of the original image.
Consider the shares as given below

Share 1: Randomly generated bits.

Share 2: XOR secret of Share 1.

The secret data are recomputed with the XOR of Share 1 and Share 2 as below.

n= 25

Secret = 11001

Share1 = 10100

Share2 = 01101

In the visual cryptography threshold scheme [2], Shamir proposed that k points are divided in to m shares such that other party requires the same m shares to get the information. If other party receives less than the m shares that is m-1 shares,

**Revised Manuscript Received on January 30, 2020.**
***** Correspondence Author

**Ashok Kumar J***, Research Scholar, Bharathidasan University,Engineering and Applications, School of Computer Science, Tiruchirappalli, Tamilnadu, India.
**Dr. Gopinath Ganapathy**, Registrar, Bharathidasan University, Tiruchirappalli, Tamilnadu, India.

they cannot retrieve the original information. This scheme is advantageous because of there is no decryption algorithm is needed and even infinite computing power will not predict the message. When all the divided shares are transmitted, attacker may receive all the shares and perform the man in the middle attack to construct the original image. But it is not possible, if they are getting m-1 shares [3]. In this proposed methodology, asymmetric cryptography such as Elliptic Curve Cryptography is used to encrypt any one of the shares and thus the attacker will not reveal the information from the encrypted data.

## III. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Neal Koblitz and Victor Miller independently proposed the ECC and is used in wireless and mobile network, etc. It is based on an Abelian group [4].

Elliptic curve E over prime field Fp denoted by E($F_p$):

$$y^2 \ mod \ p = (x^3 + ax + b) \ mod \ p$$

Weierstrass equation:

$$\Delta = (4a^3 \ + 27b^2\ ) mod \ p \ \neq 0$$

$E_p$(a,b) denotes the points for the elliptic curve over prime field Fp. The mathematical operation for Elliptic Curve Cryptography is described here.

### 3.1 Point addition

Calculating an addition of two distinct point P(x1,y1) and Q(x2,y2).

$$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$$
$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$$
$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$
$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)} \bmod p$$

### 3.2 Point subtraction

It is performed with subtracting mirror coordinates along x-axis.

$$P(x_1, y_1) - Q(x_2, y_2) = P(x_1, y_1) + Q(x_2, -y_2)$$

### 3.3 Point doubling

It is performed by addition of two same coordinates value.

$$P(x_1, y_1) + Q(x_1, y_1) = R(x_3, y_3)$$
$$x_3 = (\lambda^2 - 2x_1) \bmod p$$
$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$
$$\lambda = \frac{(3x_1^2 + a)}{(2y_1)} \bmod p$$

### 3.4 Point multiplication

It is performed by repeated addition of base coordinate point.

kP = P + P + P + · · · + k times.

## IV. RELATED WORKS

Ali Soleymani, Md Jan Nordin and Zulkarnain Md Ali proposed the methodology to map the image pixel value to the coordinate value of elliptic curve by using the table and finally encrypted with the receiver's public key [5]. S. Behnia, A. Akhavan, A. Akhshani, A. Samsudin proposed the image encryption technique to transform the plain image data matrix with the selected key into one dimensional matrix and finally encrypted and reshaped into original dimension [6].

Naor and Shamir's proposed the Visual Cryptography technique is to split the original image by encoding or decoding the original image based on Boolean matrices [7]. In the visual cryptography threshold scheme [8], Shamir proposed that k points are divided in to m shares such that other party requires the same m shares to get the information. If other party receives less than the m shares that is m-1 shares, they cannot retrieve the original information. This scheme is advantageous because of there is no decryption algorithm is needed to compute the original message.

## V. IDEA BEHIND THIS PROPOSED ALGORITHM

Consider the size of an original image of n bits which is to be transferred into public cloud. The computational cost of encrypting the whole image with ECC Algorithm is too high and so the hybrid methodology with Visual Cryptography is proposed for transferring the image in public cloud.

By using Visual Cryptographic technique, secret image can be converted into (2,2) visual secret shares. These two shares can be transferred independently into public cloud. when the two shares are available in the hands of the unknown person, then it can easily be decrypted by him.

Thus, there is no security for each share when it is combined to form original image. In order to secure each share, ECDH secret key will be used to encrypt the secret share. Thus, data confidentiality is retained in each share and data authentication process is also been achieved with this asymmetric cryptography. Once each share is encrypted with ECDH secret key, other party can do the same process of ECDH algorithm to obtain the original image. By stacking the two shares will not reveal the original image and this proposed algorithm requires the ECDH secret key for decrypting the original image. Thus, it minimized the computation cost for encrypting the whole image and transfer the secret image as Visual Cryptographic shares into public cloud on the fly with the ECDH asymmetric cryptography.

## VI. PROPOSED ALGORITHM

As seen from the above information, ECC algorithms are having limitations in encryption of huge data like images. Visual Cryptography shares are not secure if any another party obtains all shares in the unsecured channel.

Therefore, the alternate hybrid approach is proposed for Image Encryption in the public cloud. The algorithm proposed in this paper minimize the computation cost for encryption process and increases the security for visual shares.

### 6.1 Encryption Phase

### Phase I: ECDH Algorithm

a. Generate the Alice's ECC Public Key and ECC Private Key pair. Alice's public key depends upon the scalar multiplication of his private key and the generated point is on the ECC chosen curve.
b. Alice and Bob exchange their public keys and calculate the shared secret.
c. If ECDH secret key is obtained, then call Phase II with the shared secret k.

### Phase II: Visual Cryptography

d. Read the Secret Image to transfer from Alice to Bob.
e. Convert the Secret Image into (2,2) shared secret image say Secret Image Share1 IS1 and Secret Image Share2 IS2 by using Visual Cryptographic technique.
f. Secret Image Share1 IS1 is the randomly generated bits and the bits are stored in the variable b2.
g. Convert Secret Image into bits and stored it into variable b3.
h. Read 24 bits from the variable b2 , b3 and 8 bits from the ECDH key k and do XORing as defined in below operation upto the last bit in the variable b2 and b3. Finally store those result in b4.

$$b4 = b2 \wedge b3 \wedge k$$

i. *b4 is* concatenated as a single string S1 by using the base64 format. Single string concatenation is the process of making 8 bits into 6 bits base64 format.
j. b3 is concatenated as a single string S2 by using the base64 format. Single string concatenation is the process of making 8 bits into 6 bits base64 format.
k. Send base64 string s1 and s2 to Bob.

### 6.2 Decryption Phase

### Phase I: ECDH Algorithm

a. Generate the Bob's ECC Public Key and ECC Private Key pair. Bob's public key depends upon the scalar multiplication of her private key and the generated point is on the ECC chosen curve.
b. Alice and Bob exchange their public keys and calculate the shared secret.
c. If ECDH secret key is obtained, then call Phase II with the shared secret k.

### Phase II: Visual Cryptography

d. Read the base64 string s1 and s2 from Alice.
e. Convert the single string s1 and decode the base64 in to variable m2. Decoding base64 string s1 is the process of making 6 bits into 8 bits.
f. Convert the single string s2 and decode the base64 in to variable m3. Decoding base64 string s2 is the process of making 6 bits into 8 bits.
g. Read 24 bits from the variable m2 , m3 and 8 bits from the ECDH key k and do XORing as defined in below operation upto the last bit in the variable m2 and m3. Finally store those result in m4.
$m4 = m2 \wedge m3 \wedge k$
h. Original image m4 is verified by using (2,2) Visual Cryptographic Technique. If the two images are stacked properly, it reveals the Decrypted image as the original image. Otherwise, the entire process will be discarded.

## VII. IMPLEMENTATION

Elliptic curve namely "secp256k1" is known to Alice and Bob for encryption or decryption of data with the following parameters.

Finite field p : p=0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f

Coefficient a : a=0

Coefficient b : b=0

Base point G : g=(0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798, 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8),

Order n : n=0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141

Cofactor h : h=1

Key Pair Generation:

- The **private key** is a random integer d chosen from {1,..,n-1} (where n is the order of the subgroup).
- The **public key** is the point H=dG (where G is the base point of the subgroup).

If we know d and G (along with the other domain parameters), finding H is "easy". when we know H and G, finding the private key d is "hard", because it requires us to solve the discrete logarithm problem**.**

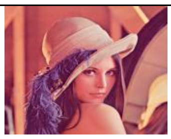
Convert the Secret Image into (2,2) shared image say Secret Image Share1 IS1 and Secret Image Share2 IS2 by using Visual Cryptographic shares.

Then XOR any one of the visual shares with the ECDH secret key k. Secret Image Shares are converted into bits and concatenated as a single string S1 by using the base64 format. It is easy to share the image based on (2,2) visual cryptography with this proposed technique and Decrypting the image is very simple.

By stacking the two shares will not reveal the original image and this proposed algorithm requires the ECDH secret key for decrypting the original image. If the two images are stacked properly, it reveals the Decrypted image as the original image. Otherwise, the entire process will be cancelled. Thus, it minimized the encryption process of image data and transfer the secret image into public cloud on the fly with the ECDH asymmetric cryptography.

## VIII. RESULTS

The proposed algorithm is implemented by using Python Language version 2.7.17 in the Lenovo Ideapad 130 core i3 7th Gen, 4GB RAM and using secp256k1 elliptic curve. Table 1 shows the time taken for the encryption and the decryption for the sample image Leena as shown in Fig I.

| Input Image: Leena.png | Output Image: Leenadec.png |
|---|---|
| |  |
| **Fig 1: Leena Image** | **Fig 2: Decrypted Image** |

**Curve**: secp256k1
**Alice's private key**:
0x7b1d56d6cfc5241b98388d99515273c63e407090102c99d5c35478da6d6760e8L
**Alice's public key:**
(0x3f6a91870eb3a1a5e38feecb1a18a9c93ebde2c4bda8bf4056fd30181bb1f319,
0xbd796e268f3fa67660369ab4f725abbb53b3cd095d398f0c51188f21529ef161)
**Bob's private key:**
0xecde8a83328928a0b7ce4b18f24ecd65f53cdf6c5289dd3f5f4160da2db26fedL
**Bob's public key:**
(0xe55bb9742606b3972a9e6ba71e9287dc85c0421f33f07f11178fbc4e16fa8217,
0xc84c5f56e673dd4fa866ba3b11eb4cca403fadbd50fc9b97bcc667bbfe0948e1)
**Shared secret:**
(0xd9af4ee038ae487c6b3577416b9ae0fd64fe03a760c9d4804aa23d9b6e79b5ef,
0xcbfb565aa3eb6be35ba2d9e8a1eee02f20ea6558c5d474ff259bd4d3b2c00f9)

**TABLE1: Time Comparison of encryption and decryption**

| Time Taken(in second) | Operations | | |
|---|---|---|---|
| | Key Generation | Encryption | Decryption |
| Our proposed method – leena image (size : 493 kb) | 0.432 | 0.625 | 0.432 |
| References [9] – leena image (size : 493 kb) | 0.03 | 8.48 | 8.20 |
| References [10] – Size : 10 kb | - | 8.964 | 3.96 |

## IX. CONCLUSION

In this paper, proposed algorithm is tested with the sample image Leena and produced the result for execution time of encryption and decryption of visual shares with the ECDH secret keys. The execution time and decryption time is compared with work of others and produced in Table I. This proposed algorithm shows minimum execution time. The result shows the intact images (Fig 2) and it is impossible to obtain the shares fully without the generated ECDH secret key.

## REFERENCES

1. Naresh vurukonda and B. Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing", Procedia Computer Science, 92, ( 2016 ), 128 – 135.
2. Divij Wadhawan, Hemank Lamba, Rajat Vikram Singh, "Visual Cryptography –Study and Implementation", https://rajatvikramsingh.github.io/media/VisualCryptography.pdf.
3. Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandee, "A Novel Image Encryption Algorithm using AES and Visual Cryptography". 2nd International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016, 808-813.
4. William Stallings, "Cryptography and Network Security Principles and Practices", 4th edition, Pearson Education Inc, 2006.
5. Ali Soleymani, Md Jan Nordin and Zulkarnain Md Ali, A Novel Public Key Encryption based on Elliptic Curves Over Prime Group Field,InJournal 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. Z. Tifedjadjine, "Halftone Image Watermarking Based on Visual Cryptography", M.Sc. thesis, Batna University, Algeria, 2005.
8. S. Chandramathi, K. R. Ramesh, R. Suresh, S. Harish, "An Overview of Visual Cryptography",International Journal of Computational Intelligence Techniques, vol. 1, no. 1, pp. 32-37, 2010.
9. Ali Soleymani, Md Jan Nordin, Azadeh Noori Hoshyar, Zulkarnain Md Ali , Elankovan Sundararajan, "An Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method" , International Journal of Digital Content Technology and its Applications(JDCTA), Volume7, Number13, Sep 2013.
10. Shruti Neralkar ; Jayashree Katti, " An Efficient Technique of Parallel Share Generation and Reconstruction for Medical Images", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, 5386-5257. 2018.