A High Secure and Robust LSB image steganography using Hybrid Encryption, LZW Compression and Knight Tour Algorithm

Archana T. Chawhan[1], Y. Manjula[2], K.B. Shivakumar[3], M.Z. Kurian[4]

PG Student (DE) Dept. of Electronics & Communication Engineering, Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, India.

Assistant Professor, Dept. of Electronics & Communication Engineering, Sri Siddhartha Institute Of technology, Tumakuru, Karnataka, India.

Professor, Dept. of Tele-Communication & Engineering, Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, India.

HOD, Dept. of Electronics & Communication Engineering, Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, India.

Abstract: The challenge of steganographic method is to create a rational balance between the quality of the file and size of the data that can be transferred. In addition, the robustness of the technique and security of the obscure data are the facts that cannot be dissembled. The Least Significant Bit (LSB) insertion approach provides a high degree of visual quality and a large amount of capacity for the concealed data, but the converted message is not well protected in this method. In the proposed method, the secret data is firstly encoded by using the AES encryption method to guarantee the protection of the hidden message. Then the Lempel Ziv Welch (LZW) technique compresses the data to reduce the occupational capacity of the confidential data. Then, by utilizing the extended Knight Tour algorithm, each bit stream of the data is spread out on the image to increase the robustness of the method. The prominent feature of the proposed method is it not only improves the security and payload capacity problems of the simple LSB method, but also increases the visual quality of the stego image. On comparing the results of the proposed method with the base paper improvements may be seen. Selecting the better encryption method taking the comparisons of AES and ECC method is also considered.

Keywords: Steganography, AES, ECC, LZW compression and Knight tour algorithm

I. INTRODUCTION

Data protection and security of the personal information have become a critical issue in the digital world. Therefore, the demand of having a protected method to transfer the confidential data is dramatically increasing. The steganography which literally means “covered writing”[2] is a branch of cryptography and is the art and science of communicating in a way which hides the existence of the communication. Steganography can be applied electronically by taking a message and some sort of cover and combining both to obtain a “stego-object”. In contrast to cryptography which make data unreadable for a third party by implying some encryption methods, steganography emphasize on hiding the existence of message inside another data in such a way that nobody can detect it.

Image Steganography Evaluation Parameters:When a large amount of data is embedded into an image the visual specifications

of image such as colour and smoothness area altered[3]. Based on this fact that steganography is the process of hiding the important information inside a cover data without arising the suspicious, it is very important to specify how the secret data is embedded in the image. There are some essential factors that should be considered in image steganography process.

- Capacity: Refers to the maximum number of bits that can be embedded in a particular cover file with a small probability of revealing by an antagonist.
- Imperceptibility: Is defined as the degree of changes in the appearance of the cover data whenever the message is embedded.
- Robustness: Indicates the distortion amount that the digital cover can tolerate to keep the message safe.
- Security: Denotes the assurance of keeping the secret data unreadable for the adversary when it is extracted by attacks.

II. RELATED WORK

"Digital image steganography: Survey and Analysis of current methods" by A. Cheddad[2] presented a novel which contains the different steganography methods. Currently 3 methods are used. First is Spatial domain method which has encoding at the level of LSB. Second is Frequency domain which as different kind of transformations i.e. DCT, DFT etc. Third is Adaptive steganography which takes the statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The statistics will dictate where to make the changes.

"On the limits of Steganography" by R.J. Anderson and F.A.P. Petitcolas[3] described techniques for concealing meta information about a message such as its eexistance, duration, sender and receiver are collectively known as traffic security.Theoretical limits of Steganography contains several parameters that are perfect compression, entropy, selection channel, the power of parity and equivalence.

"Hiding data in images by simple LSB techniques" by C.K. Chan and L.M. Cheng[4] proposed a technique by applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution. By this method the quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived.

"A more secure steganography method in Spatial Domain" by A. Daneshkhah[5] presented a method in which two bits of message is embedded in a pixel in a way that not only the least significant bit of pixel is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated. But the point is in each embedding process only once alteration in one bit plane is allowed to happen. As it is compared by the method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.

"An LSB Data hiding using Prime numbers" by S.Dey[6] presented data hiding technique using prime and natural numbers.Fibanocci decomposition technique used to generate a different set of virtual bit-planes all together, thereby increasing the number of bit-planes all together, thereby increasing the number of bit-planes. There are two approaches to generate virtual bit-planes. First is based on decomposition of a number in sum of prime numbers. LSB, fibanocci, prime number and natural number techniques has 8,12,15,23 bit-planes respectively.

"Approximate string matching on Ziv-Lempel compressed text" by J. Karkkainen[7] described string matching on Ziv-Lempel compressed text. Given a text of length u compressed into length n, and a pattern of length m, we repeat all the R occurrences of the pattern in the text allowing up to K insertions, deletions and substitutions. The general idea is to replace substrings in the taxt by a pointer occurrence of them.

"A pseudo-random number generator for personal computer" by I.M. Sobol and Y.L. Levitan[8] proposed a pseudo random number generator. The random variable Gamma is an ideal mathematical abstraction. There are no true variable Gamma in reality. Therefore as a rule, in computers pseudo random numbers if they are computed from a prescribed formula but satisfies different requirements as I they were true random variables.

"An efficient algorithm for the Knight's tour problem" by I. Parberry[9] presented a algorithm for the knight's tour problem is a series of moves made by a knight visiting every square of an nxn chessboard exactly once. The solution for this problem is divide and conquer method. The 2 rectangular compartments are called as Quadrisected knight's tour algorithm.

III. PROPOSED SYSTEM

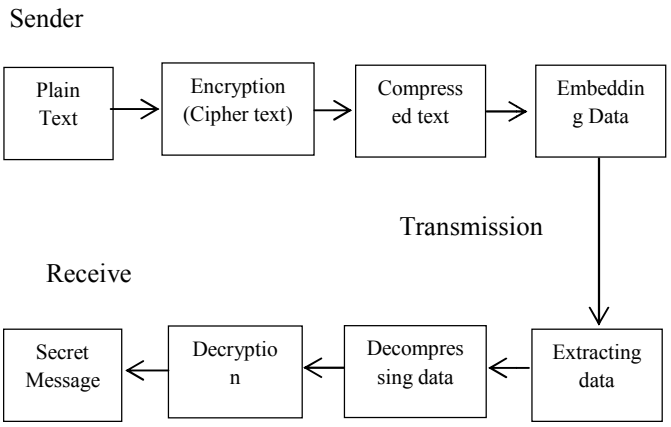


Fig: Proposed system design

a. Embedding Process

This phase includes all the activities that must be carries out to hide and protect the secret data inside the cover image. The sender uses some algorithms to encode and compress the data and then embeds the bit stream into the image.The sending process consists of following procedures:

1.Encryption – In the first step of the ambedding phase, the plin text will be encrypted using different Encryption algorithms.

i.AES(Advanced Encryption Standard) Algorithm: This algorithm is flexible in supporting any combination of data and key size of 128, 192 and 256 bits. However, AES[10] merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks organized as a 4x4 matrix that is called the state. For full encryption, the data is passed through number of rounds Nr (Nr=10,12,14)

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse bounds are applied to transform cipher text back into the original plaintext using the same encryption key.

- **Sub Byte transformation:**In the sub byte transformation step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, $S;b_{ij}=S(a_{ij})$.

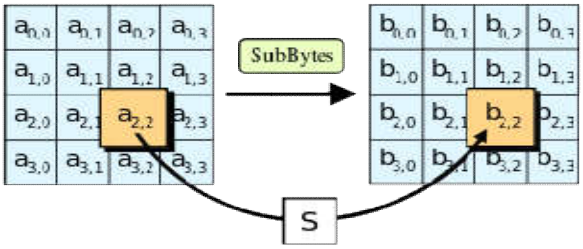


Fig: Sub Byte transformation

- **Shift Rows Operation:** In the shift rows step, bytes in each row of the state are shifted cyclically to the left. The number of places each bytes shifted differs for each row. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third row and fourth rows are shifted by offsets of two and three respectively.

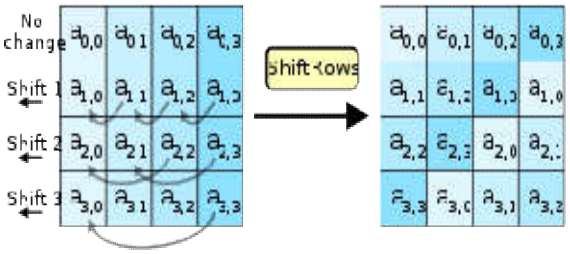


Fig: Shift Rows operation

- **Mix Columns Step:** In the Mix Columns step, each column of the state is multiplied with a fixed polynomial c(x). In this step four bytes of each column of the state are combined using an invertible linear transformation.

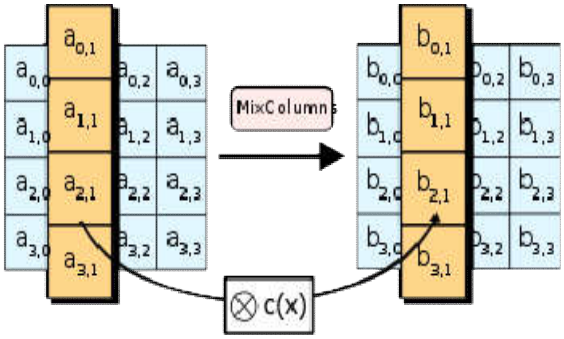


Fig: Mix Columns operation

- **Add Round Key operation:** In this step each byte of the state is combined with a byte of the round subkey using the XOR operation.Here the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule.

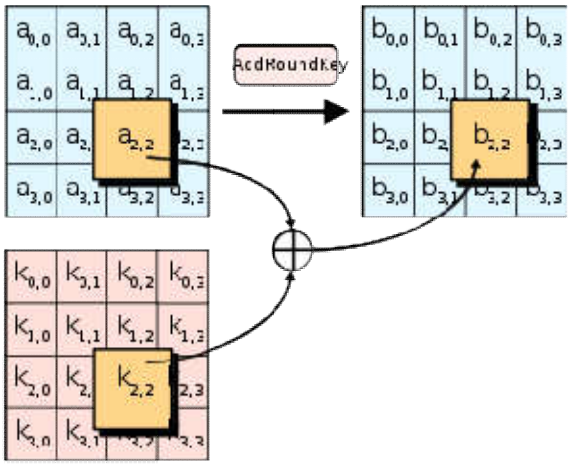


Fig: Add Round key operation

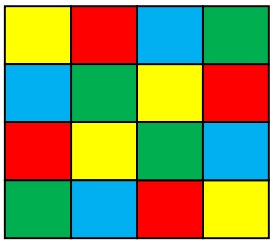
ii.ECC (Elliptic Curve Cryptography): An Elliptic Curve Cryptography(ECC) technique, which is an approach to public-key cryptography bsed on the algebraic structure of elliptic curves over finite fields. The entire security of ECC depends on the ability to compute point multiplication. The size of the elliptic curve defines the difficulty of the problem. The ECC gaining popularity because it offers similar security to traditional systems, such as Ron Rivest, Adi Shamir, and Leonard Adleman(RSA), but with significantly smaller key size, reducing storage and transmissions requirements than RSA based system. For current cryptographic system, an elliptic curve is a plane curve which consists of points satisfying the equation (1).

$$y^2=x^3+ax+b \bmod p \qquad (1)$$

to use ECC, all parties must agree on all the elements defining elliptic curve i.e. the domain parameters of the scheme. The field is defined by P in the prime case and pair of m and f in the binary case. The elliptic curve is defined by the constants a and b used in its defining equation. Finally, the cyclic subgroup is defined by its generator point G. For cryptographic application the order of G i.e. the smallest value of n such that nG=0 is a prime number.

2.Compression – Compression method is employed effectively to diminish the size of the message. LZW creates a table to replace the repetitive succeeding characters with binary code. This table, which is known as dictionary, will be sent to the recipient the end of the compression process to be used for extracting original secret message.

3.Embedding – The embedding algorithm is the most prominent part of the steganographic methods. In fact, it defines which pixels of the image should be change and also in what order they will be altered with the secret data. The Knight tour algorithm is a suitable technique to formulate the sequence of the secret bit stream within the image pixels. The advantage of the knight tour is that it is self-developed algorithm based on the knight tour mathematical problem[9] and it is almost unknown for the unintended receivers. By considering the image as a extended chessboard, we can have a algorithm, which determines the path of the knight within the image. The solution of the "Knight Tour" problem divides the chess board into the blocks with size of 4x4 squares. Also, it considers four groups of four squares in each block namely "Right diamond", "Left Diamond", "Right Square" and "Left Square".



Yellow=Left Diamond

Green=Right Diamond

Red=Left Square

Blue=Right Square

The main rule of the surfing is to complete all the squares within the chess board on each group (colour) and then move to the next group of squares.

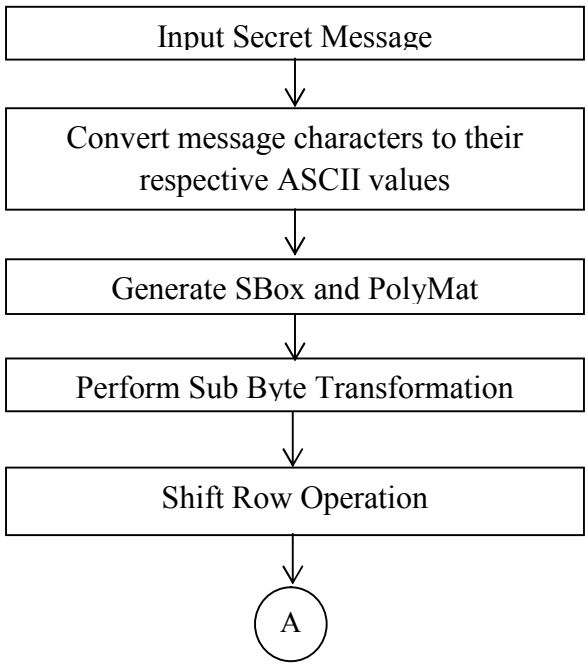
b.Extraction Phase

On the other side of the communication line, the receiver should be able to comprehend the secret data within the Stego-image. Therefore, another procedure is required to recover the content of the message and restructure it.

First of all, based on the stego-key and the extracting algorithms (the same as sender side) the bits of the secret message are obtained to compose a compressed data. Then the unzipping algorithm will generate the encrypted data and finally, by AES decryption the plain message will be revealed.

IV. SYSTEM IMPLEMENTATION

AES Encryption: AES operates 4X4 column major matrix of bytes termed as state. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plain text, into the final output, called the cipher text. The Sub Byte transformation, Shift row, Mix Columns and the Add Round Key Operations are performed on the secret message.



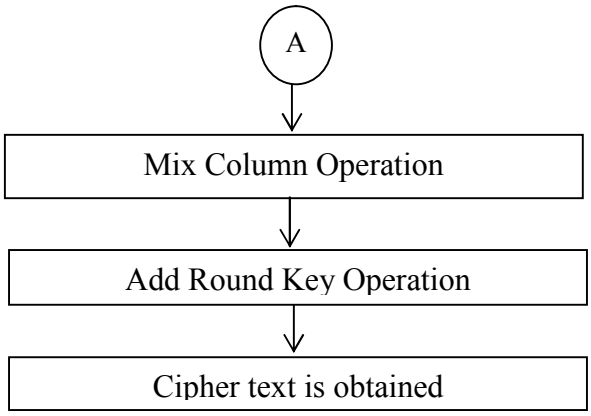


Fig: Flowchart of AES

LZW Compression: LZW creates a table to replace the repetitive succeeding characters with a binary code. This table, which is known as dictionary, will be sent to the recipient at the end of the compression to be used for extracting original secret message. Advantages of LZW compression technique are LZW requires no prior information about the input data stream, it is simple and allows fast execution.

Knight Tour Algorithm: Knight Tour Algorithm is a self-developed algorithm based on the knight tour mathematical problem and it is almost unknown for the unintended receivers. By considering the image as an extended chessboard, we can have an algorithm, which determines the path of knight within the image.

a) Consider the image width and height divisible by four(Ignore the extra pixels).
b) Divide the image into 4x4-pixel blocks.
c) Go to the first pixel, which has been specified by the steg0-key and start with one group (color) and traverse all the block.
d) To move from one block to the next one, all the 4 squares must traversed.
e) If the movement for one group (color) has finished, start with the next group.
f) Repeat the steps to traverse all the pixels.
g) Replacement: When the sequence of the target pixels is defined in the previous step, now it's the time to replace the least significant bits of the image pixels with the bit stream of the secret message.

ECC: An Elliptic Curve Cryptography (ECC) technique, which is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The ECC works as per the flowchart.

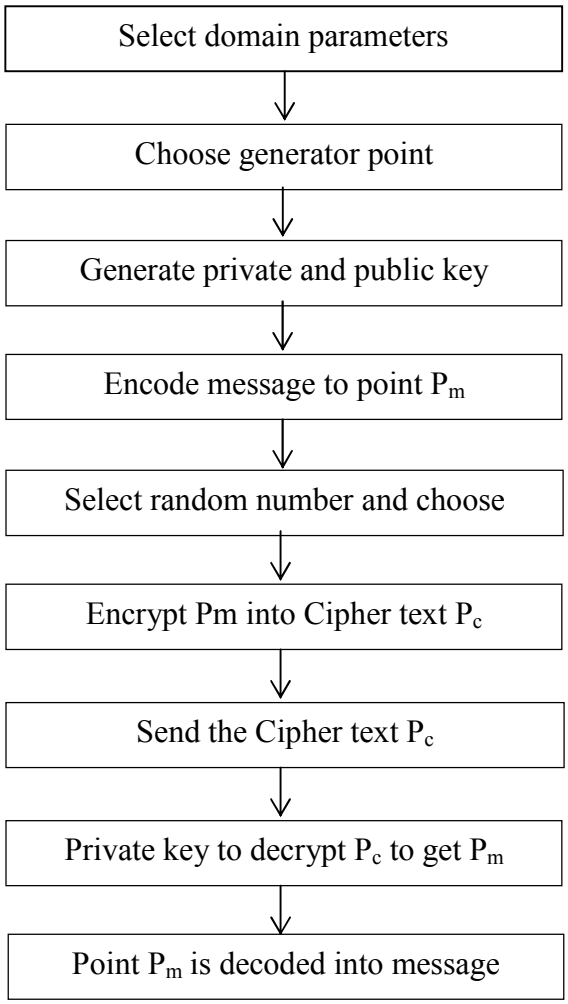


Fig: Flowchart of cryptographic implementation

V. EXPERIMENT RESULTS

The proposed system is developed using MATLAB programming. During execution, the proposed system first selects the encryption technique i.e. 1 for ECC and 2 for AES encryption.

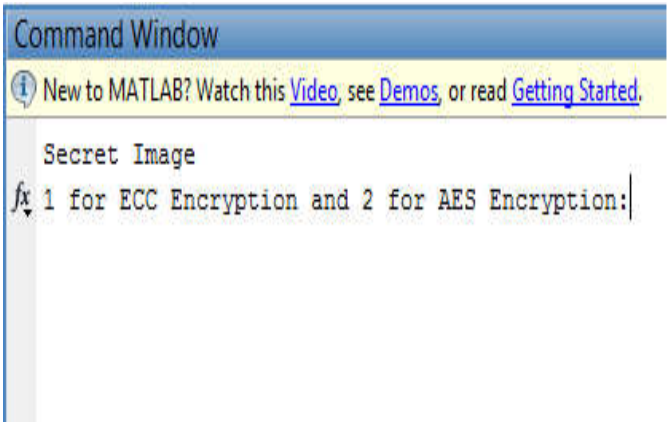


Fig: Selecting encryption technique

After selecting the Encryption technique, the message which is to be hidden is taken and converted into cipher form and this cipher text will be compressed using LZW compression technique.

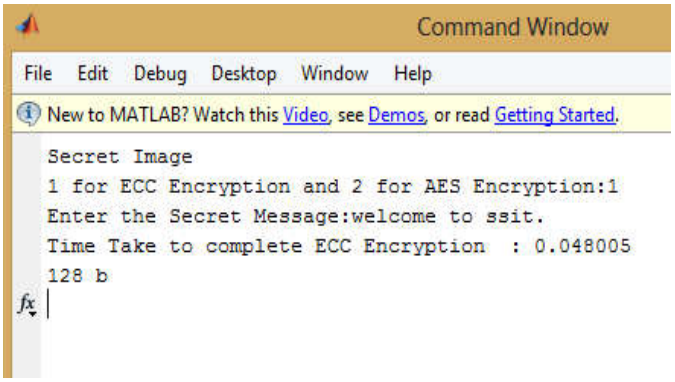


Fig: Encryption using ECC

After this the cover image in which the secret message is going to hide is selected.

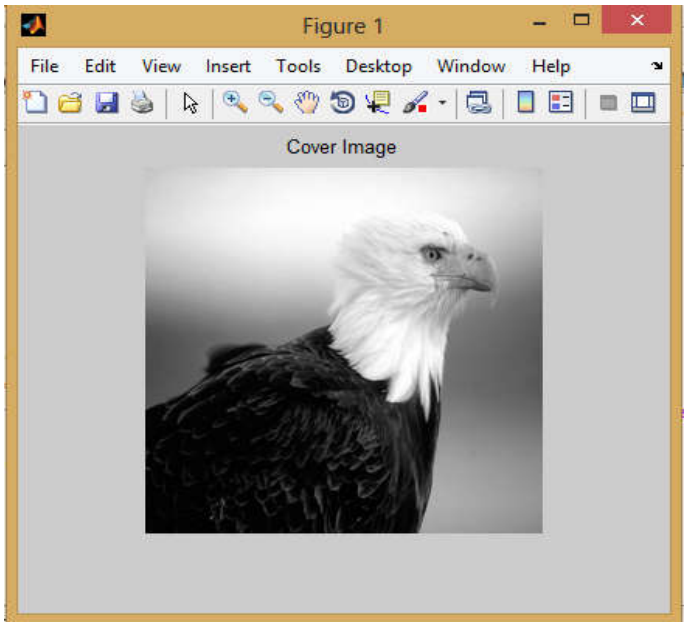


Fig: Selecting Cover image

Then the compressed text is embedded in the cover image using knight tour algorithm. This results as the Stego image that contains the secret message in its pixels. The PSNR value is displayed. The below figure shows embedding using Knight Tour algorithm and the Stego image.

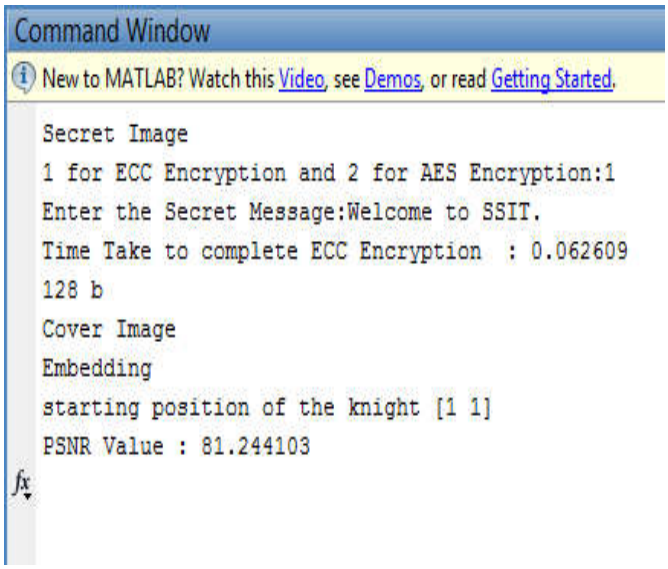


Fig: Embedding using Knight tour algorithm and displaying the PSNR value.

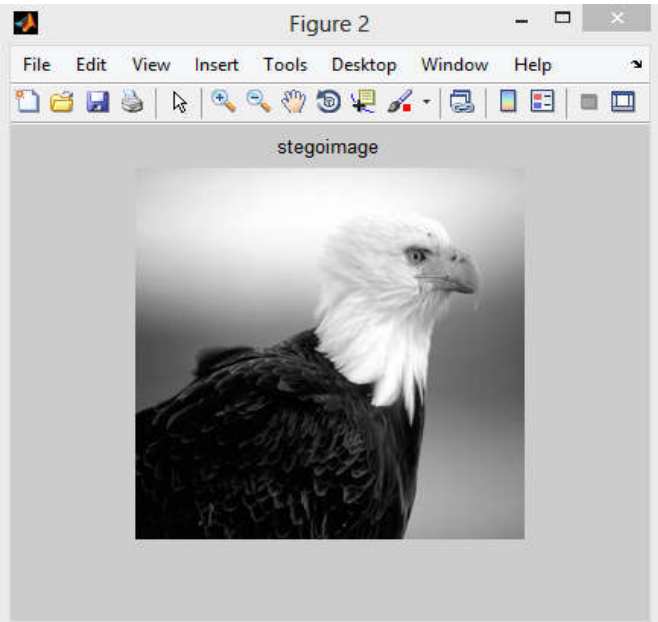


Fig: Stego image

Similarly for AES encryption 2 is selected. In the proposed method 128 bit key AES is used. First it takes the secret message then the 4 operations are performed on the message for about 10 times. Finally will get the Cipher text. This text is compressed and then embedded in the image by using Knight tour algorithm. Below figure shows the result for AES.

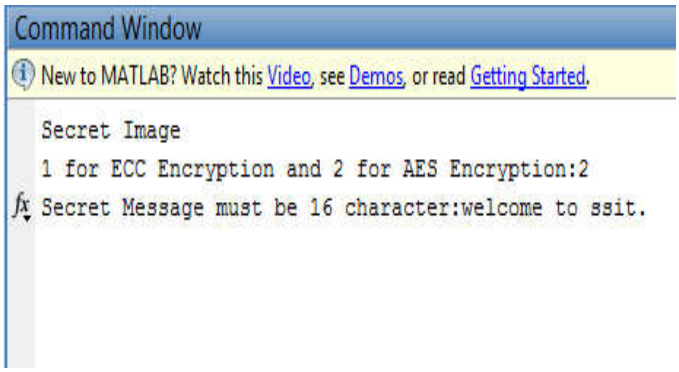


Fig: Selecting AES and giving input

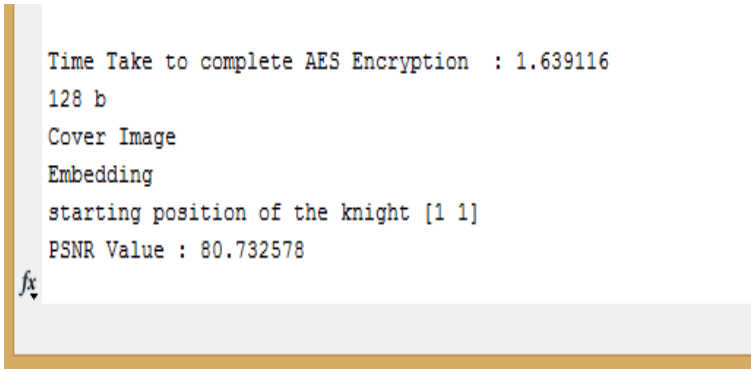


Fig: Results of AES encryption and displaying PSNR value

The below table shows the value of PSNR and the time taken to complete the encryption by the two encryption techniques for different size of data.

Data to be Encrypted in bits	ECC		AES	
	PSNR	Time taken	PSNR	Time taken
80	82.871	0.022	81.110	1.221
128	80.854	0.046	80.732	1.639
192	79.763	0.062	79.483	2.450
280	78.891	0.077	77.753	3.423
336	78.442	0.089	76.950	3.982
384	77.783	0.095	76.753	4.082
456	76.950	0.107	75.361	4.962

VI. CONCLUSION

It can be concluded that, anew method of LSB image Steganography using Hybrid encryption, LZW compression and Knight Tour algorithm is implemented. ECC encryption is compared with the AES encryption, which showsElliptic Curve Cryptography provides greater security and more efficient performance than the Advanced Encryption Standard.

REFERENCES

1. MortezaBashardoost, Ghazali Bin Sulong and ParisaGerami, “Enhanced LSB image steganography method by using Knight tour algorithm, Vigenere encryption and LZW compression” IJCSI International Journal Of Computer Science Issues, Vol. 10, Issue 2, No 1 March 2013.
2. A.Cheddad,etal.,“Digital image steganography: Survey and analysis of curretntmehods”, Signal processing, vol.90, pp.727-752,2010.
3. R.J. Anderson and F.A.P. Petitcolas, “On the limits of steganography”, Selected areas in Communications, IEEE Journal on, vol.16, pp.474-481,1998.
4. C.K.Chan and L.M.Cheng, “Hiding data in images by simple LSB substitution”, pattern Recognition, vol. 37, pp.469-474,2004
5. A. Daneshkhah, et al., “A more secure steganography method in spatial domain”, in Intelligent systems, Modelling and simulation(ISMS),2011 Second International Conference on 2011, pp.189-194.
6. S.Dey, et al., “An LSB data hiding technique using prime numbers”, in Information Assurance and security, 2007. IAS 2007. Third International Symposium on 2007, pp.101-108.
7. J. Karkkainen, et al., “Approximate string matching on Ziv-Lempel compressed text”, Journal of Discrete algorithms, vol.1,pp.313-338,2003.
8. M.Sobol and Y.L.Levitan, “A pseudo-random nmber generator for personal compters”, Computers & amp; Mathematics with Applications, vol.37, pp.33-40,1999.
9. I. Parberry, “An efficient algorithm for the Knight’s tour problem,” Discrete Applied Mathematics, vol.73, pp.251-260,1997.
10. National Institute of Standards and Technology (NIST), “Advanced encryption standard (AES)”, Federal Information processing standards publications (FIPS PUBS) 197-26,2001.