International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 4 Issue 1 January 2018

Improved Method for Data Hiding Using Stenographic Algorithm

Ketki Pande
Research Scholar
Department of CSE, LNCT Bhopal
ketkiupadhyay22@gmail.com

Dr. Vineet Richhariya
Professor & Head
Department of CSE, LNCT Bhopal
vineetrich100@gmail.com

Abstract— The rise of technology especially in the field of computer science has opened the door of opportunity to handle images in variety of ways to best apt for the situation such as while capturing, processing, storage and transmitting. The wide spread use and growth of World Wide Web has enabled users to efficiently transmit or access data from virtually any place. As the amount of data comprising image grows bigger and bigger, it will render itself useless in the absence of any effective method to access and use it. There are many potential problems in relation to effective search and navigation that can be solved through the use of efficient information retrieval system. In steganography, before the hiding process, the sender must select an appropriate message carrier, an effective message to be hidden as well as a secret key used as a password. A robust stenographic algorithm must be selected that should be able to encrypt the message more effectively. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. The receiver after receiving the message decrypts the hidden message using the extraction algorithm and a secret key. This paper proposes a new algorithm to hide data inside an image using stenographic technique. The algorithm that we have proposed is an enhanced version of LSB technique that is not very much robust. Also we have implemented a compression technique to increase the hiding capacity.

Keywords— Steganography, Data hiding, LSB, RRBE, PSNR.

I. INTRODUCTION

Steganography has its vicinity in protection and privacy. It isn't meant to update cryptography however decorate it. Hiding a message with Steganography methods decreases the threat of a message being detected. If the message is encrypted then it provides every other layer of safety .Therefore, some Steganography methods combine conventional Cryptography with Steganography [1]; the sender encrypts the secret message prior to the general communique system, as it is very tough for an attacker to detect embedded cipher textual content in a cover [2].

In the sphere of Steganography, a few terminologies have evolved. The adjectives 'cowl', 'embedded', and 'stego' had been described on the records hiding workshop held in Cambridge, England. The term "cover" refers to description of the unique massage, facts, audio, video, and so on. Steganography isn't a brand new technological know-how, it dates returned to past times [3].

II. LITERATURE SURVEY

In [4] a hybrid data hiding technique is presented in which LSB data hiding technique is used with a key permutation to hide data. In this paper focuses on capacity and security, in LSB data hiding technique data hide in the LSB bit of the host image and in this paper a optimal LSB substitution based data hiding technique is presented

In [5] a decomposition base LSB data hiding technique is presented in which no bit planes are generated in which more data can be stored that enhance the capacity of the image. In this paper comparison among techniques like casual LSB data hiding technique, Fibonacci based LSB technique, prime no. based LSB technique, and natural no. based LSB technique is presented in which natural no based decomposition LSB technique is performed better than others.

In [6] adaptive least significant bit based technique is presented, which resolves the problem of existing techniques which used hide data in image edge area parameter to hide data but generate deformity in the shape of the image. In Adaptive LSB edge brightness and texture masking of image to estimate the pixel to hide data pixels in noisy non sensitive regions are embedded with k pixels of the k LSB bits which used to hide data it take larger values of k pixels as compare to noisy regions. A pixel arrangement method is used to rearrange the pixel to enhance the visual quality of stego-image, it enhance the capacity and imperceptibility of the image. Further for future, a lossless watermark framework can be implemented to enhance visual quality of image.

In [7] Data hiding has recently been proposed as a promising technique for the purpose of information assurance, authentication, fingerprint, security, data mining, and copyright protection, etc. lossless data hiding technique based on histogram modification, this technique uses difference of adjacent pixels to insert data and enhance the capacity of the system. No. of message bit inserted in the image are equal to no. of peak pixels a histogram modification is used to prevent overflow and underflow of the pixels, that technique takes the

property of color image, that a color image has 3 times more capacity as compare to gray scale image in that this technique uses difference of adjacent pixels rather than plane pixels to embed message with image, thus it enhance the capacity of the image

Literature Review In [8] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

III. PROPOSED WORK

Early techniques to image Steganography were not basically based on visual features but based on the textual annotation of images. This means initially the images were first annotated with text and then later were searched using text-based approach seen in typical traditional database management system. This trivial method of image retrieval is very sensitive to the keywords employed by the user and the system. Therefore, LSB has received much attention in multimedia retrieval community. It deals with the image content itself such as color, texture, and shape and image structure instead of annotated text.

LSB is used to analyze image information using low level features of image like color layout, color, shape and texture. LSB is also used to create feature vectors of an image as its index. Image feature database is used to store features for future reference. Image query is given in this method to retrieve image. The features are extracted from the query image and are used to match it against features from the feature database using a pre-established algorithm. This helps the system retrieve group of similar images to the query image can be returned as the retrieval images [9].

Basically, one of the key points of realizing LSB is to extract appropriate feature vectors to represent image content correctly. Color is low-level visual feature that is extensively used since it is invariant to image size and orientation. Similarly since Color histogram is invariant to orientation and scale, it becomes a powerful in image classification. It is this reason, color histogram-based color descriptors have not only been subject of extensive research, but they are also used in LSB system for the sake of simplicity and effectiveness.

The work discussed in literature contains the different approach for data security which increase the key length and provide the data security, the further approach can apply to enhance LSB to E LSB technique for the proposed work along with the symmetric key encryption technique which provide the high resolution with low computation time for the encryption and decryption as compare to other approach.

Methodologies/Algorithm Details

Blowfish Algorithm:

Algorithm used for generating symmetric keys which maintains data security.
This algorithm has 16 rounds.
The input is a 64-bit data element, d.

1) Divide d into two 32-bit halves: d1, d2.
2) Then, for n = 1 to 16:
d1 = d1 XOR Xn
d2 = F (d1) XOR d2
3) Swap d1 and d2
4) After the sixteenth round, swap d1 and d2 again to undo the last swap.
5) Then, d2 = d2 XOR X17 and d1 = d1 XOR X18.
6) Finally, recombine d1 and d2 to get the cipher text.

Least Significant Bit Algorithm: algorithm Used for embedding the secret message with image. Each frame or image is made up of no of individual pixels. Each of these pixels in an image is made up of a string of bits the 4least significant bit of 8-bit true color image is used to hold 4-bit of our secret message image by simply overwriting the data that was already there.

1. In hiding process, the last 4 bits of image or frame pixel is replaced with 4 bits of our secret data.
2. For this secret data which is also sequence of bytes are broken down into set of
   4 bits. To hide each character of secret message we need two pixels. So the number of characters that we can hide in (mx m) image is given by the following equation.
   Total size of one frame 8 ——————————— -(1)

1) Suppose size of a single frame is 160KB, then for 1LSB, maximum data that can be hidden is 120KB = 20KB. For 2LSB it is 220KB = 40KB. For 3LSB it is 3x20=60KB. For 4LSB it is 420KB =80KB. If stenographic process go beyond 4LSB, i.e. for 5LSB it is 520KB=100 KB, means that size of the data can be hide is more than 50
2) For implementing steganography proposed method is using 4LSB algorithm. Any data

change in least significant bit does not change the value of data significantly.

The complete algorithm for the encoding model and decoding model is performed using which the data security can be obtain via cryptography and steganography approach.

Blowfish Algorithm:

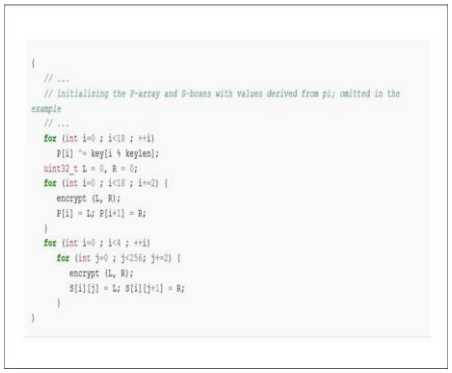


Fig1: Blowfish Algorithm

Proposed system is reversible, that is data extraction and image recovery is without any loss. If we reverse the order of encryption and vacating room, i.e., Firstly vacate room and then image encryption at owner side means reserving room before encryption (RRBE).Proposed system uses three algorithms namely:

1. RDH(Reversible Data Hiding)
2. LSB(Least Signicant Bit)
3. HS(Histogram Shift)

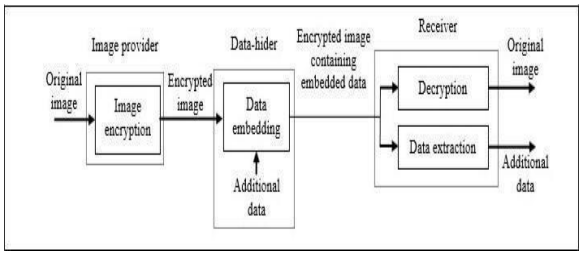


Fig.2: Architecture diagram

Modules description

Lossless Data Hiding Scheme
Reversible Data Hiding Scheme
Combined Data Hiding Scheme

Lossless Data Hiding Scheme:

A lossless data disguising plan for open key-mixed pictures is proposed. There are three get-togethers in the arrangement: a photo provider, a data hider, and a gatherer. With a cryptosystem having probabilistic property, the photo provider scrambles each pixel of the principal plaintext picture using individuals when all is said in done key of the beneficiary, and a data hider who does not know the primary picture can change the figure content pixel-qualities to embed some additional data into the encoded picture by multi-layer wet paper coding under a condition that the unscrambled estimations of new and one of a kind figure content pixel regards must be same.

While having the mixed picture containing the additional data, a recipient knowing the data covering key may expel the embedded data, while a gatherer with the private key of the cryptosystem may perform disentangling to recoup the principal plaintext picture.

The embedded data can be isolated in the encoded zone, and can't be removed subsequent to unraveling since the unscrambled picture would be same as the primary plaintext picture as a result of the probabilistic property

Reversible Data Hiding Scheme:

This portion proposes a reversible data covering get ready for open key-encoded pictures. In the reversible arrangement, a preprocessing is used to withdraw the photo histogram, and after that each pixel is encoded with included substance holomorphic cryptosystem by the photo provider.

While having the mixed picture, the data hider changes the figure content pixel regards to embed a bit-course of action created from the additional data and slip-up cure codes. Due to the holomorphic property, the modification in encoded space will realize slight augmentation/reduce on plaintext pixel regards, deriving that an unscrambling can be executed to get a photo like the main plaintext picture on authority side.

Because of the histogram contract before encryption, the data embedding operation does not cause any surge/undercurrent in the direct decoded picture. By then, the main plaintext picture can be recovered and the embedded additional data can be expelled from the particularly unscrambled picture.

Joined Data Hiding Scheme

A lossless and a reversible data covering gets ready for open key-encoded pictures are proposed. In both of the two designs, the data embedding operations are performed in encoded zone.

On the other hand, the data extraction philosophy of the two designs are through and through various. With the lossless arrangement, data introducing does not impact the plaintext substance and data extraction is in like manner performed in encoded space. With the reversible arrangement, there is slight bowing in particularly

unscrambled picture caused by data embedding's, and data extraction and picture recovery must be performed in plaintext territory.
That surmises, on authority side, the additional data introduced by the lossless arrangement can't be expelled in the wake of unscrambling, while the additional data embedded by the reversible arrangement can't isolated before deciphering.
In this fragment, we unite the lossless and reversible intends to fabricate another arrangement, in which data extraction in both of the two spaces is achievable.

Blowfish algorithm:

- Using blowfish algorithm for encryption and decryption.
- Which provides symmetric key at sender and receiver side?
- An authentication, privacy is provided whenever transmitting secrete data.
- Blowfish generates 64 bit symmetric key iteratively which is difficult enough to crack by attacker**.**

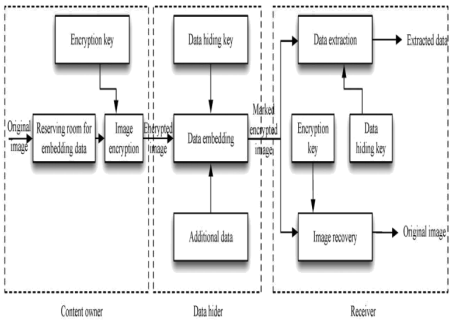
Working of Blowfish algorithm [10]:

It involves basic three steps which are:

1. Divide 64 bit data into 2 equal partition as left and right, XOR left side with p size array.
2. Implement F function which includes divide 32 bit into 4 subparts called as S-block XOR each of them and combine them all to get final result for function F.

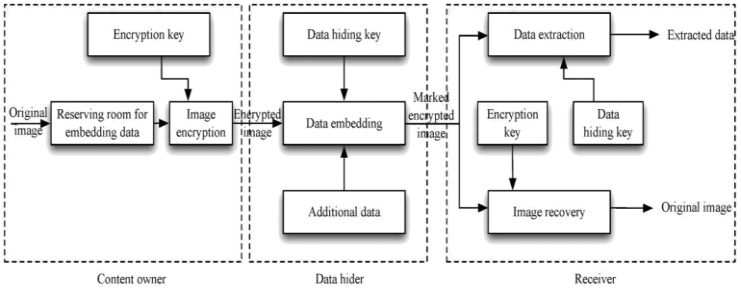
3. XOR right part of 32 bit called it as F' now iteratively swapping the values will result to final asymmetric key generation which will be a key for encryption**.** Lossless data hiding is providing a way better security with combination of LSB algorithm and Blowfish algorithm for sensitive data transmission.

The method first vacate room and encrypt the data to target image and pass embedded image to receiver side where receiver extract its data from image without any loss.



Reserving Room Before Encryption Framework

Paper ID: IJETAS/January/2018/07



Reserving Room Before Encryption Framework

Fig.3: Encryption Framework

Advantages of Proposed System

- We can perform data encryption back side of image.
- We can easily hide the large amount of data background of image.
- High performance without data loss.
- Free from any error.
- No image distortion.
- Gives PSNR (peak signal to noise ratio) value**.**

IV. RESULT ANALYSIS

To check the feasibility of the proposed recuperation structure this zone deals with the purposes of enthusiasm of execution appraisal that fuses the photo database, the evaluation estimations, and the delayed consequence of proposed system and execution examination with existing procedures.

- **Image Database**

The image dataset is downloaded from the different image resource. This image database consists of 64 X 64 objects.


Pirate

Fig.4: Example of Image Dataset [11]

Our proposed estimation is performed using JDK 8.0 API, where the Utilized system setups as Windows 10 OS, 4 GB

Methodology	4LSB	PSNR	Accuracy
Enhanced proposed System	80	90	90.6
Proposed System	70	76	65
Existing System	60.5	52.5	35

RAM, 750 GB hard circle, i3 processor. The examination performed on net beans IDE and count is executed on different pictures. In the wake of playing out the result examination on figuring with LSB and Canny edge revelation and steganography on it. The going with results was procured by performing test using LSB and Proposed figuring.

- **Evaluation Matrices**

Keeping in mind the end goal to ascertain the adequacy of our approach PSNR in DB are figured as: PSNR is most effortlessly characterized by means of the mean squared blunder (MSE).Given a noise-free *m*×*n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

- **Graphical User Interface (GUI)**

Java Swings or Graphical User Interface Design Environment was used for building the Graphical User Interface. Following graphical UI,, for LSB application was arranged by using the outline gadgets gave by Swing portions:

- **Retrieval Results**

The proposed technique on the previously mentioned picture database is actualized. In addition test on a similar database utilizing the technique proposed in past work, is led with the end goal of examination. The trial brings about terms of PSNR in DB and limit utilizing proposed technique and the other three strategies are appeared in Table 1 and Table 2 separately

Table 1: results are analyze by using Existing algorithm model.

The table mentioned above provides the result of comparison between existing and the proposed algorithm.

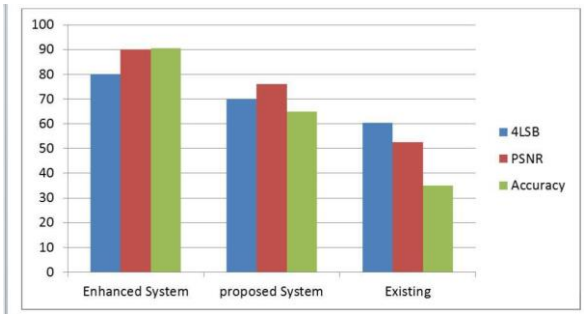


Fig5: comparison analysis bar graph between existing and proposed technique.

- **Implementation Details**

In order to perform the experiment implementation the Java API **Abstract Window Toolkit**. It is a portable GUI library between Solaris and Windows 95/NT and Mac System 7.X (soon) for stand-alone applications and/or applets. Since it can be used in applets it can be used on IRIX, SunOS, HP/UX, and Linux which Netscape 2.0 supports.

The Abstract Window Toolkit provides many classes for programmers to use. It is your connection between your application and the native GUI. The AWT hides you from the underlying details of the GUI your application will be running on and thus is at very high level of abstraction. It takes the lowest common denominator approach to retain portability. No floating toolbars or Balloon helps here...

It is a Java package and can be used in any Java program by importing java.awt.* via the **import** keyword. The documentation for the package is available at the Java home page. The package will be covered briefly as this document is not considered advanced material because it does not discuss Peers, Image Consumers/Producers, Toolkits and other advanced AWT ilk. It is recommended you look at the source code to see how the AWT really works.

As per discussed about the proposed work, further implementation to outperform the execution and algorithm being implemented by us is mentioned and run using Java API, net beans IDE platform using the SWING API concepts, where the event handling is perform to execute each component operation and the output is show in the further figure.

Fig 6.- Loading of initial screen

In the figure 6 above the initial loading screen is shown where the components related to data conversion and tool which are going to use it. The JMenu option is used to display three option embed the message in image and further another option to retrieve the message from the steganography image.

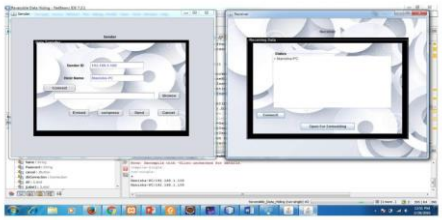


Fig 7: Selection of the base image and output image.

In the figure above the selection for the base image on which the data is going to hide, also selection of output file on which hidden data is going to obtain.

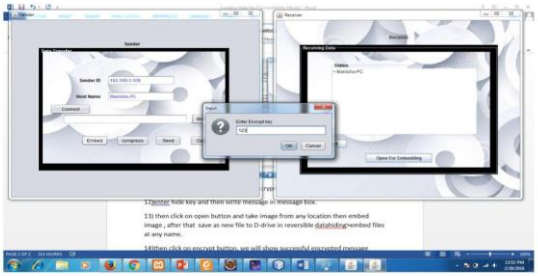


Fig 8: Selection of the algorithm and selection of the Key

In the figure above, the selection of the performing algorithm and alongside the algorithm password can be taken for the data security encryption purpose. Further the data in text format is given and then the output image is generated.

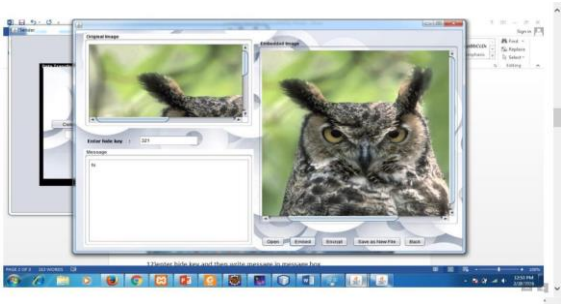


Fig 9: output file generation and message embedding screen.

In the figure above the output file is generated where the message text given is embedded and the dialog is shown where the message printed for the same.

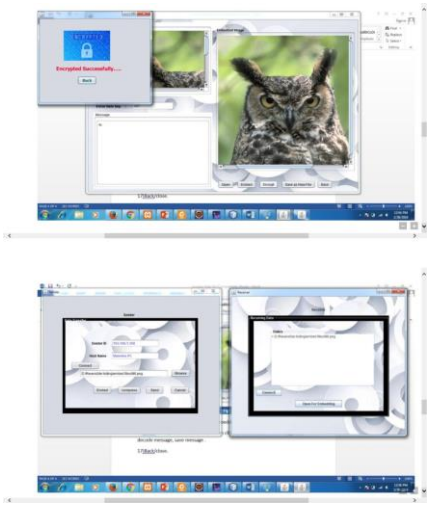


Fig 10: Information retrieval phase, message status phase.

In the figure 10 above the retrieval phase is taken into consideration, where the master image in which the message is hidden, encrypted status and furthers the operation requested and data retrieval process is given a choice to perform operation.

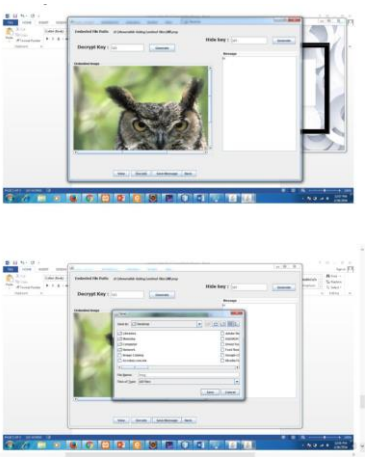


Fig 11: De-steganography and decryption phase using key and reverse process.

In the figure 11 above the screen states that the message can be retrieve upon giving the key and selection of reverse process.

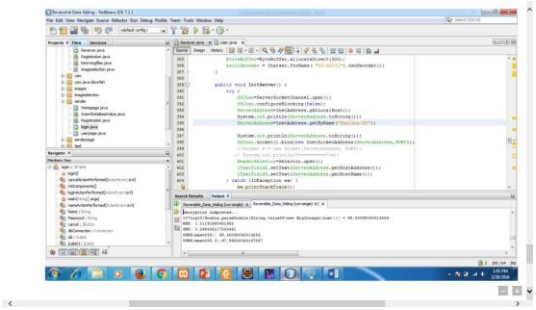


Fig 12 :parameter PSNR for result retrieval

In the figure 12 in the course of the last recuperation side operation and result procured is communicated where the figure express that the embedded message is recouped from the expert picture and result is appeared on help which is gotten ensuing to performing steganography. Along these lines the whole utilization contain the methodology, for instance, – Loading of the crucial screen, introducing stage and a short time later recuperation organize, where each one of the three strategies play out the aggregate execution.

CONCLUSION

Data Security is an important concept of research where number of data transmission occur in different format of data. Textual and multimedia data is the key concept of any data propagation sharing among the unit. There are many image securities and steganography concept is presented in the existing work which discuss about the secure data transmission. In this Dissertation conclude that, the prevention of data attack is reduced and data security is provided at greater extend. Total loss data recovery is possible at the time of data extraction. The given solution is based on the enhancement to LSB (least significant bit) approach, which is a data hiding approach. Further A secure symmetric key based encryption algorithm which is Blowfish algorithm is proposed by work. Thus a combine approach for providing data security and data sharing is presented. cryptography with probabilistic and holomorphic properties. The proposed work is implemented using the Java API, where the Swing API and file system is used for experiment evaluation. Some standard image data is used for experiment purpose. The conducted experiment and result evaluation shows the efficiency of proposed algorithm while comparing with the existing solution.

References

[1] Ashadeep Kaur, Rakesh Kumar and Kamaljeet Kainth, "Review Paper on Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol 6, Issue 6, ISSN: 2277 128X,June 2016.

[2] Mehdi Hussain and Mureed Hussain, " A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology (IJAST), Vol 54, May 2013.

[3] Hemang A. Prajapati and Nehal G. Chitaliya, " Secured and Robust Dual Image Steganography: A Survey", International Journal of Innovative Research in Computer and Communication Engineering, Vol 3, Issue 1, January 2015.

[4] Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed and Ki-Hyun Jung Symmetry 2016, 8(6), 41; doi:10.3390/sym8060041

[5] IBM SNA Formats Bit Ordering is Opposite of Intel Convention. Microsoft. 2014-02-23.

[6] Masoud Afrakhteh, Jeong-A Lee First published: 12 March 2014DOI: 10.1002/sec.998

[7] Yun Q. Shi1, Zhicheng Ni1, Dekun Zou1, Changyin Liang2and Guorong Xuan New Jersey Institute of Technology, Newark, NJ, USA, shi@njit.edu2Shenzhen Polytechnic, Shenzhen, China 3Tongji University, Shanghai, China

[8] BLionel Fillatre ICD LM2S, Université de technologie de Troyes, UMR STMR CNRS 6279, Troyes, France.

[9] Announcing the ADVANCED ENCRYPTION STANDARD (AES) (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.

[10] B. Schneider. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993). Springer Verlag, 1994, pp. 191-204.

[11] YFCC100M Dataset. mmcommons.org. Yahoo-ICSI-LLNL. Retrieved 1 June 2017.