# A Review Paper on Images, Steganography and Crytography

Deepti Upadhyay[1], Dr. Satyaranjan Patra[2], Ms. Smita Rani Biswal[3]

[1,2,3]*Computer Science& Engineering*

[1]*Bhopal Institute of Technology & Science,* [2]*Bhopal Institute of Technology & Science, Bhopal*

[3]*Padmanava College of Engg., Rourkela*

***Abstract — The rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. In this concern images are play an important role of exchanging information. Digital images are widely communicated over the internet. The security of digital images is an essential and challenging task on shared communication channel. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this research paper, we are going to review the steganography and different type of images along with the cryptography techniques.***

***Keyword — Steganography, Images, Cryptography, Information Security, Data Hiding.***

## 1. INTRODUCTION

For the perception of data security it is more important to protect data from outside the privilege area. Internet had eased the way of transferring data and communicating with other users. In this digital world, a user's personal/banking information may need to be shared with other internet users via the social applications. This information, if not secured, can be intercepted by malicious users vulnerable to illegal use. Also, the security of the secret information in defense and other applications is of major concern. Therefore to protect information from an unauthorized access, we need robust security mechanisms. In this manner security of data is of foremost importance in today's world. Security has become one of the most important factors in communication and information technology [1] [2].

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party [3].

## 2. BACKGROUND

Since the inception of internet the security of information is the most vital factor in information technology and communication. Therefore, the background of a study is an important part of our research paper. It provides the context and purpose of the study. Hence there is need for background study that contribute to prepare proposed system.

### 2.1 What is Steganography?

Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. The word steganography comes from the Greek Steganos, which mean covered or secret and – graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [4] and a communication is happening [5]. Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

### 2.2 Different Types of Steganography

Increased use of internet, information becomes available on-internet, a person who possesses an internet can easily get data from internet for information that they want [6]. The use of steganography techniques can be broadly classified in four types which is depict in given diagram:

**Use Text:** Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every $n^{th}$ letter of every word of a text message.

**Image:** Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

**Audio/Video:** To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably

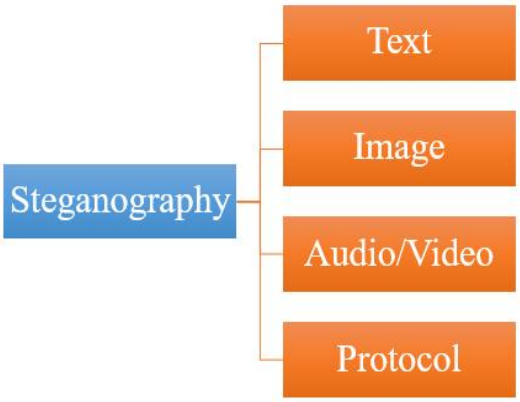


**Figure 1. Categories of steganography**

**Protocol:** The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [7].

### 2.3 Image Cryptography

In these days as multimedia data transferred over insecure channel, it becomes an important issue to encrypt image with a suitable image encryption algorithms. An image encryption is different from text due to large processing, pixels definition, time to encrypt and size. This is also a different approach due to different type of attacks possible on text and image data. With the ever-increasing growth of multimedia applications, important issue for communication and storage of images is security, and encryption is one the technique to ensure security. encryption techniques convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the confidential message without a key for decryption [8].

Image cryptography algorithms attempt to convert original images to other images that are difficult to understand in order to keep the image confidentiality between users. In other words, it is important that without a key for decryption, nobody could get to know the content. Majority of traditional algorithms are basically used for encryption of text data; however they do not fit for the multimedia data particularly images due to their huge size. Furthermore, decrypted text result should be similar to the original text, while decrypted image is not required to be similar with original image [9].

## 3. BASICS OF IMAGE

An image, digital image, or image is a computer generated graphic or picture that appears on-screen. In terms of the image processing and computer application that is representable with the 2D array or vector. These array or vectors are contains some values and known as pixels, these values are varying between 0-255 of combinations. And using the combination of these values the real world information is stored. One way to describe an image using numbers is to declare its contents using position and size of geometric forms and shapes like lines, curves, rectangles and circles; such images are called vector images [2].

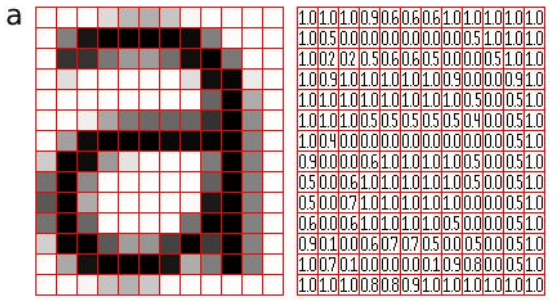


**Figure 2. Bitmap Images**

A vector image is resolution independent, this means that you can enlarge or shrink the image without affecting the output quality. Vector images are the preferred way to represent Fonts, Logos and many illustrations. Bitmap-, or raster, images are “digital photographs”, they are the most common form to represent natural images and other forms of graphics that are rich in detail. Bitmap images are how graphics is stored in the video memory of a computer. The term bitmap refers to how a given pattern of bits in a pixel maps to a specific colour.

A bitmap images take the form of an array, where the value of each element, called a pixel picture element, correspond to the colour of that portion of the image. Each horizontal line in the image is called a scan line. The letter 'a' might be represented in a 12x14 matrix as depicted in Figure 2. The values in the matrix depict the brightness of the pixels (picture elements). Larger values correspond to brighter areas whilst lower values are darker. When measuring the value for a pixel, one takes the average colour of an area around the location of the pixel. A simplistic model is sampling a square, this is called a box filter, and a more physically accurate measurement is to calculate a weighted Gaussian average (giving the value exactly at the pixel coordinates a high weight, and lower weight to the area around it). When perceiving a bitmap image the human eye should blend the pixel values together, recreating an illusion of the continuous image it represents [2].

8bit:

A common sample format is 8 bit integers, 8bit integers can only represent 256 discrete values ( = 256), thus brightness levels are quantized into these levels.

12bit:

For high dynamic range images (images with detail both in shadows and highlights) 8 bits 256 discrete values does not provide enough precision to store an accurate image. Some digital cameras operate with more than 8bit samples internally, higher end cameras (mostly SLRs) also provide RAW images that often are

12 bit ( bit = 4096).

16bit:

The PNG and TIF image formats supports 16 bit samples, many image processing and manipulation programs perform their operations in 16bit when working on 8bit images to avoid quality loss in processing.

Floating point:

Some image formats used in research and by the movie industry store floating point values. Both "normal" 32bit floating point values and a special format called half which uses 16bits/sample. Floating point is useful as a working format because quantization and computational errors are kept to a minimum until the final render.

### 3.1 Category of Images

Pictures are the most common and convenient means of conveying or transmitting information. A picture is worth a thousand words. Pictures concisely convey information about positions, sizes and inter-relationships between objects. They portray spatial information that we can recognize as objects. Human beings are good at deriving information from such images, because of our innate visual and mental abilities. About 75% of the information received by human is in pictorial form [3]. There are 3 category of digital images are as following.

Binary:

Binary images are useful for fingerprints, architectural plan, and text (printed or handwriting. This images use only two color black and white. It require only 1 bit per pixel for storage. This images also known as two-level or bi-level and store as bitmap in memory.

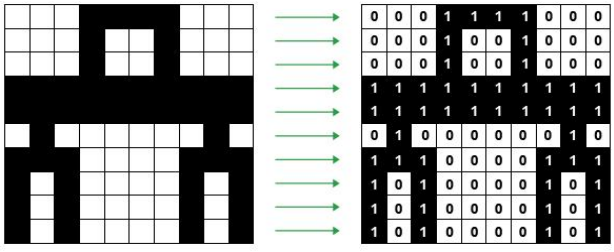


**Figure 3: Binary Image**

Gray-Scale:

Gray-Scale images suitable for recognition of natural objects, printed work images, Diagnostic photography using X-ray. In this type of images pixels range is between black and white. In 8 bit representation 256 states are available. These images are different from black-and-white images which have just two color black and white. Gray-Scale images have shades of gray between black and white colors.

**Figure 4: Gray-Scale Image**

True colour or RGB

An RGB colour image is M*N*3 array of colour pixels where each colour pixel is equivalent to third component of RGB image. The three components of RGB image is referred as red, green, blue module images. The data class of RGB image determines the range of values and this image is of class double range between [0, 1]. The range values of this image are [0,255] or [0, 65535] for RGB images of class unit16 respectively. The pixel value of the component image verifies the bit depth of the RGB image for instance, if each component image is 8-bit image then analogous RGB image is said to be 24 bit deep. In this case, the number of possible colours in an image is (2^b) ^3, where b is the number of bits in each component image for 8-bit case, the number is 16,777,216 colour.

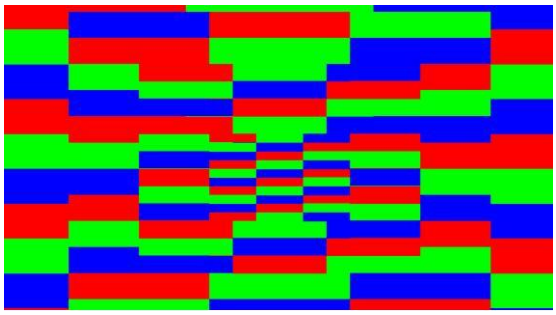

**Figure 5: RGB Image**

### 3.2 Information Hiding

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

In addition, the rapid growth of publishing and broadcasting technology also require an alternative solution in hiding information. The copyright such as audio, video and other source available in digital form may

lead to large-scale unauthorized copying. This is because the digital formats make possible to provide high image quality even under multi-copying. Therefore, the special part of invisible information is fixed in every image that could not be easily extracted without specialized technique saving image quality simultaneously [4]. All this is of great concern to the music, film, book and software publishing industries.

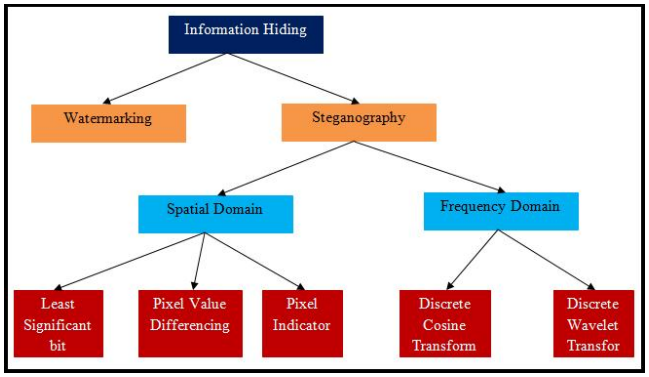


**Figure 6: Disciplines of information hiding [4]**

Figure 6 shows various disciplines of information hiding. Hiding information in audio files can be done by using frequencies that are inaudible to human ear. Similarly, video files can also be thought of to embed secret information. Since it is a moving stream of images and sounds, any minor distortions may be unseen because of continuous flow of information. The advantage in this case will be high payload capacity. Image is the most popular file format used for steganography as they possess high degree of redundancy. With image steganography, better imperceptibility and payload capacity can be achieved. Steganalysis is an art of detecting covert communication [5].

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography [6]. All these applications of information hiding are quite diverse [7].

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.

Steganography hides the secret message within the host data set and presence imperceptible. In those applications, information is hidden within a host data set and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an informal analysis

## 4. CRYPTOGRAPHY

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography [30].

One essential aspect for secure communications is that of Cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck [30].

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext [31].

### 4.1 Classification of Cryptography

One should be cautious that each cryptographic key is used for the particular purpose it is designed for. If the same key is used for other purposes (which often occurs), much damage or loss of security may result [32] [33]

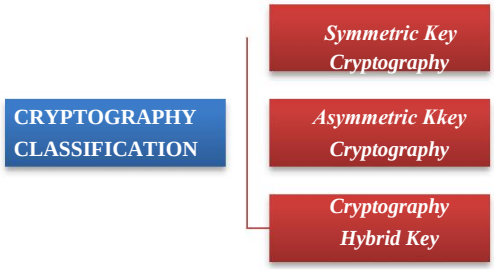


**Figure 7 Cryptography Classification**

Cryptography can be divided into three major category based on the use of key.

Symmetric Encryption (Private Key Encryption): In this type of encryption same key is used at the time of

encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption. Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key. A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. Substitution maps each plaintext element into cipher text element, but transposition transposes the positions of plaintext elements. Example: DES, 3DES, BLOWFISH, AES etc.

Asymmetric Encryption (Public Key Encryption): In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts. ; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is extremely difficult or impossible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key, asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other application that never is implemented using symmetric encryption. Example: RSA algorithm.:Hybrid Encryption (Combination of private and public): Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message.

### 4.2 Image Cryptography

In these days as multimedia data transferred over insecure channel, it becomes an important issue to encrypt image with a suitable image encryption algorithms. An image encryption is different from text due to large processing, pixels definition, time to encrypt and size. This is also a different approach due to different type of attacks possible on text and image data. With the ever-increasing growth of multimedia applications, important issue for communication and storage of images is security, and encryption is one the technique to ensure security. encryption techniques convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the confidential message without a key for decryption [35].

Image encryption means to prepare an image from an image that is difficult to understand, and recognize. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption [34].

Image encryption algorithms attempt to convert original images to other images that are difficult to understand in order to keep the image confidentiality between users. In other words, it is important that without a key for decryption, nobody could get to know the content. Majority of traditional algorithms are basically used for encryption of text data; however they do not fit for the multimedia data particularly images due to their huge size. Furthermore, decrypted text result should be similar to the original text, while decrypted image is not required to be similar with original image [36].

Image encryption algorithms can be categorized into full encryption and partial encryption (also called selective encryption) based on the sum of encrypted data. According to the percentage of the encrypted data, unfortunately, the time for processing of encryption and decryption is the main concern in real-time image communication. Time can be categorized into two levels, one for encryption time and another for time for transferring images. The first step is to choose a robust, fast and easy method to implement in order to reduce the time. Encryption and decryption algorithms are not fast enough to deal with the enormous amount of transmitted data. A significant criteria relating to the method is to decrease the image encryption size and maintain quality of the image. Partial Encryption is a suitable method to encrypt only the lowest portion of data to lessen the computational requirements of enormous amounts of multimedia data. It is essential to lessen the

images encryption time in distributed network by minimizing the sum of data to encrypt and attaining a reasonable security and minimizing the computation. The implementation of partial encryption just started in 1990's.

### 4.3 Characteristic of Cryptography

Although some important characteristics might not be quantifiable, it seems intuitively logical that it should be possible to identify some cryptographic algorithm characteristics that can be expressed either in objective, numeric values or subjective, adjectival values. Metrics might be used for evaluating and comparing cryptographic algorithms and the inferred confidentiality protection value of products containing cryptographic algorithms.

## 5. CONCLUSION

Information security is greatly essential over the unsecured shared medium. Due to the exponential growth of internet users, unauthorized access of information has become one of the most significant problems. Therefore, to provide more security to the information at the time of communication over unsecured channel, image steganography, an advance technique for data security is needed. On the basis of above point, in this review paper, we have reviewed the steganography with its background and different type of images along with the cryptography techniques.

## REFERENCES

[1] Saritha, M., Vishwanath M. Khadabadi, and M. Sushravya, "Image and text steganography with cryptography using MATLAB", 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), IEEE, 2016, pp. 584-587

[2] Clerk Maxwell, "Digital image representation", available online at: http://pippin.gimp.org/image_processing/chap_dir.htm

[3] Kit A. Peterson, "Introduction to Basic Measures of a Digital Image for Pictorial Collections", Digital Conversion Specialist, June 2005.

[4] N. Provos, "Probabilistic Methods for Improving Information Hiding", CITI Technical Report 01-1, January 31, 2001

[5] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital image steganography: survey and analysis of current methods, Signal Process, 90 (2010), PP.727–752.

[6] H. Wang, S. Wang, Cyber warfare: Steganography vs. steganalysis, Communication ACM 47 (2004) PP.76–82.

[7] R an Isbell, "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, 10 May 2002.

[8] Muhalim Mohamed Amin "Information Hiding Using Steganography", e-thesis, Universiti Teknologi Malaysia, 2003.

[9] Komal Patel and Sumit Utareja, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications (IJCA), Volume 63– No.13, February 2013.

[10] Sumeet Kaur, Savina Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", International Conference on Computing for Sustainable Global Development, IEEE 2014.

[11] R. Popa,"An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[12] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[13] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[14] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[15] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.

[16] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[17] "Reference guide: Graphics Technical Options and Decisions", http://www.devx.com/projectcool/Article/19997

[18] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.

[19] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[20] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[21] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004

[22] C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.

[23] S. Tanako, K. Tanaka and T. Sugimura, "Data Hiding via Steganographic Image Transformation", IEICE Trans. Fundamentals, volume E83-A, pp. 311-319, February, 2000

[24] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[25] Prof. S. V. Kamble, Prof. B.G. Warvante, "A Review on Novel Image Steganography Techniques", IOSR-JCE-2004

[26] Nadiya, P.V.; Imran, B.M., "Image steganography in DWT domain using double-stegging with RSA encryption," Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on , vol.7, no. 8, pp.283,287, Feb. 2013.

[27] Anjali Tiwari, Seema Rani Yadav and N.K. Mittal,

[28] "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 7, January 2014

[29] Ayushi, "A Symmetric Key Cryptographic Algorithm",

International Journal of Computer Applications, PP. 1-4, Volume 1, No. 15, 2010.

[30] M.Kundalakesi, Sharmathi.R and Akshaya.R, "Overview of Modern Cryptography", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (1), PP. 350-353, 2015.

[31] Manoj Kumar Pandey, Mrs. Deepty Dubey, "Survey Paper: Cryptography The art of hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), PP. 3168-3171, Volume 2, December 2013.

[32] Prakash Kuppuswamy, and Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review: An International Journal, Volume 19, No. 2, PP. 1-13, March 2014

[33] Lahieb Mohammed Jawad and Ghazali Bin Sulong, "A Review of Color Image Encryption Techniques", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013

[34] Nitin Rawal and Manoj Dhawan, "A Survey Report on Image Encryption Techniques", International Journal of Engineering Research & Technology (IJERT), Volume 2, October 2013.

[35] Norman D. Jorstad, Landgrave T. Smith Jr, "Cryptographic Algorithm Metrics", Directorate for Freedom of Information and Security Review (OASD-PA) Department of Defense, January 1997

[36] Phad Vitthal S. and Bhosale Rajkumar S, "A Novel Security Scheme for Secret Data using Cryptography and Steganography", I. J. Computer Network and Information Security, 2012, 2, pp. 36-42

[37] Rajalakshmi C S, Sowjanya.TP and Hemanthumar C S, "Image Steganography using H-LSB Technique for Hiding Image and Text Using Dual encryption method", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – Volume 2 Issue 5 – May 2015

[38] S. Mohanapriya, "Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 5, May 2012

[39] Ketki Thakre and Nehal Chitaliya, "Dual Image Steganographyfor Communicating High Security Information", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-3 July 2014

[40] Zhou, Xinyi, Wei Gong, WenLong Fu, and LianJing Jin, "An improved method for LSB based color image steganography combined with cryptography", 2016 IEEE/ACIS 15th International Conference on, Computer and Information Science (ICIS), pp. 1-4, 2016.