International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 1, January 2015, PP 113-120
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Data Security by Riversible Data Hiding Process

Supriya M. Diwe[1], Manisha Mokade[2], Anjali R. Keude[3], Deepika R. Paunikar[4], Eshan G. Motghare[5]

Student, Department of Computer Engineering
Bapurao Deshmukh College of Engineering, Sewagram, India
[1]supidiwe@gmail.com, [2]mokademanisha@gmail.com, [3]anjalikeude@gmal.com,
[4]paunikardeepika123@gmail.com, [5]Dmotghare52@gmail.com

Prishita S. Mahiskar[6]

Professor, Department of Computer Engineering
Bapurao Deshmukh College of Engineering, Sewagram, India
[6]Dprishita976@gmail.com

Abstract: *As we are living in an electronic world. The advancement in World Wide Web and the explosive growth in communication techniques in recent years have created a lot of conveniences in our day to day life. Here we have to give prime importance to the security and the confidentiality of data which we have to keep safe. Data hacking is a very challenging problem in today's internet world. There are number of methods to secure data such as substitution, permutation etc. so in this paper we proposed a technique to hide data in image by using reversible data hiding technique with double protection to the secret data .*

In this technique the data or files which are very confidential can be hidden into an image which is made a watermark image by applying the traditional RDH (Reversible data hiding algorithm and then that image is encrypted by using ECC algorithm. But there is still insecurity that if the hackers get that image than he can get the data from that image, he will try some algorithms on it. So to confuse the hacker from its work we are proposing the system with an additional advantage in that. After encryption the again that image is converted into the text format and then send to the target. So if the hacker gets some information about some kind of encryption than he tries to solve it, but as he doesn't know whether it is a text or an image he won't be succeeded. He tries to overcome the data by using some coading but as all the confidential data is hidden within that image he will never know this. And in this way you can provide double security to the data inside. This is mostly used in forensics, military imagery, medical imagery etc.

Keyword: *Watermarking, stenography, data hiding, ECC algorithm.*

1. Introduction

As we are living in an electronic world, the advancement in World Wide Web and the explosive growth in communication techniques in recent years have created a lot of conveniences in our day to day life. Here we have to give prime importance to the security and the confidentiality of data which we have to keep safe. Data hacking is a very challenging problem in today's internet world. There are number of methods to secure data such as substitution, permutation etc. so in this paper we proposed a technique to hide data in image by using reversible data hiding technique with double protection to the secret dataThere are many possible ways to transmit data using the internet: via emails, chats, etc. However, one of the main problems with sending data over the internet is the "security threats it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.You can save or send your data in an open way, just put a password on it and send. And what if the people are hackers or identity thieves. It's not enough to encrypt your document. For real protection, you have to hide in plain sight images. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet in order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher textsand transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats. So we have introduced a method of reversible data hiding in encrypted images by reserving room before encryption. That means hiding the data in within an image.

2. LITERATURE REVIEW

Besteena K , Philumon Joseph 2 in 2014 in the paper ”Secure Reversible Data Hiding in Encrypted Images By Reserving Space In Advance” , proposed the method can achieve real reversibility, that is, data extraction and image recovery are free of any error. It can be used in situations where both image and data have equal importance [1].

Shilpa Sreekumar, Vincy Salam in 2012 in the paper “Advanced Reversible Data Hiding with Encrypted Data” proposed the advanced RDH work focuses on both data encryption and image encryption which makes it more secure and free of errors. All previous methods embed data without encrypting the data which may subject to errors on the data extraction or image recovery. The proposed work provides a novel RDH scheme in which both data and image can be encrypted and extracted reversibly without any errors. In the proposed work, data extraction and image recovery are free of any errors. The PSNR is significantly improved in the proposed work. This advanced work also performs data hiding in videos [2].

In February 2014 Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade Hide Inside-Separable Reversible Data Hiding in Encrypted Image In this paper, we propose a novel method by reserving memory space before encryption with a traditional RDH technique, and thus it is easy for the data hider to reversibly embed data in the image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error [3].

Yanli Ren, and Zhenxing Qian in 2012 in the paper “Scalable Coding of Encrypted Images In the encryption phase”, the original pixel values are masked by a modulo-256 addition with pseudorandom numbers that are derived from a secret key. After decomposing the encrypted data into a down sampled subimage and several data sets with a multiple-resolution construction, an encoder quantize the subimage and the hardman coefficient of each data set to reduce the data amount. Then the data of quantized subimage and coefficient are regardless as a set of bit streams. At the receiver side, while subimage is decrypted to provide the rough information of the original content, the quantized coefficients can be used to reconstruct the detailed content with an iteratively updating procedure. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bit streams are received [4].

Harish G, SmithaShekar B, Prajwal R, Sunil S Shetty in july 2014 in the paper “Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption” All previous methods embed data by reversibly vacating room from the encrypted images, which may subject to some errors on data extraction and/or image restoration. Here, a novel method is proposed so as to reserve room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility [5].

Harshitha K M, Dr. P. A. Vijaya in June 2012 in the paper “Secure Data Hiding Algorithm Using Encrypted Secret message” proposed a combination of steganography and cryptography, which provides a strong backbone for its security. The scenario of present day of information security system includes confidentiality, authenticity, integrity, non-repudiation. This present work focus is enlightening the technique to secure data or message with authenticity and integrity. The entire work has done in MATLAB. The hidden message is encrypted using a simple encryption algorithm using secret key and hence it will be almost impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key. Only receiver and sender know the secret key. N-bit LSB substitution technique is used as embedding and extraction method. This method could be most appropriate for hiding any secret message (text, image, audio, and video) in any standard cover media such as image, audio [6].

In April 2012 “Data Hiding in Image using least significant bit with cryptography” by Mr. VikasTyagi proposed a technique to increase the security of messages sent over the internet steganography is used. This paper discussed a technique used on the LSB (least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it [7].

Minya Chen, Edward K. Wong, NasirMemon and Scott Adams in the paper “Recent Developments in Document Image Watermarking and Data Hiding” proposed that with the proliferation of digital media such as images, audio, and video, robust digital watermarking and data hiding techniques are needed for copyright protection, copy control, annotation, and authentication. While many techniques have been proposed for digital colour and gray scale images, not all of them can be directly applied to binary document images. The difficulty lies in the fact that changing pixel values in a binary document could introduce irregularities that are very visually noticeable. Over the last few years, we have seen a growing but limited number of papers proposing new techniques and ideas for document image watermarking and data hiding [8].

Deepthi C in Highly Secured Reversible Data Hiding in AES Encrypted Images by Reserving Room before Encryption with Authentication proposed that RDH in the encrypted images by allocating memory before encryption method is used to recover the original cover without any loss & errors. It is basically used in the medical metaphors, military metaphors and law forensics, where no distortion of the original image is allowed [9].

3. Existing System

In the existing system reversible data hiding technique the image is compressed and Encrypted by using the encryption key and the data to hide is embedded in to the image by using. The data hiding key. At the receiver side he first need to extract the image using the encryptionKey in order to extract the data and after that he’ll use data hiding key to extract the embeddedData. It is a serial process and is not a separable process.

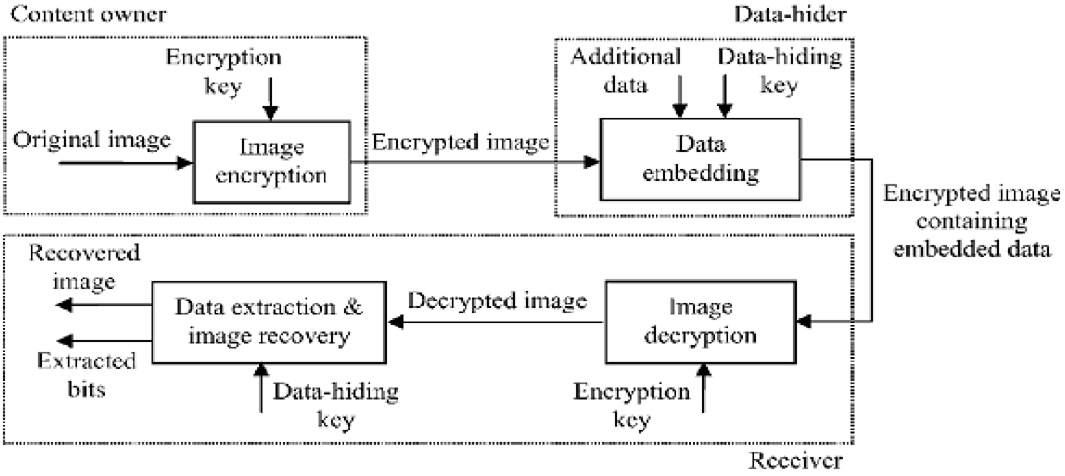


Fig3.1. *Sketch of non-separable reversible data hiding in encrypted image.*

3.1. Disadvantages

There are some drawbacks for this system which are as follows:

- Principal content of the image is revealed before data extraction.
- If someone has the data hiding key but not the encryption key he cannot extract anyInformation from the encrypted image containing additional data.

To overcome tis obstacles we have proposed a system of reserving room before encryption and converting that encrypted image into a text format.

4. Proposed System

4.1. Reversible Data Hiding

Reversible data hiding (RDH) in images is a technique, by which the original message or cover can be losslessly recovered after the embedded message is extracted. Reversible data hiding is a technique which enables images to beauthenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. This technique of authentication can be called as watermarking. For hiding any data in an image we have to first convert that image into watermark.

Fig4.1.1. *original Image*

Fig4.1.2. *Watermark Image*

The U.S. Army also is interested in this technique for authentication of reconnaissance. Image encryption is nothing but the original image is converted into pixel format and it is denoted by the number of rows and columns. But while encryption distortion at the time of data extraction is a main problem. So reversible data hiding in encrypted images is used, so that we can hide the data inside that image by encryption and also regain the original image.

It should be noted that steganography is different from watermarking technique. Watermarking is not used to transmit a secret message but to embed data, which might be visible, to guarantee ownership.

4.1. Creating Room

Reversible data hiding (RDH) in images is a special algorithm that not only guarantees the confidential data will be extracted accurately but also allows the original cover image to be reconstructed without distortion after the confidential data are completely extracted. For this khelker has proposed a technique of reserving room before encryption

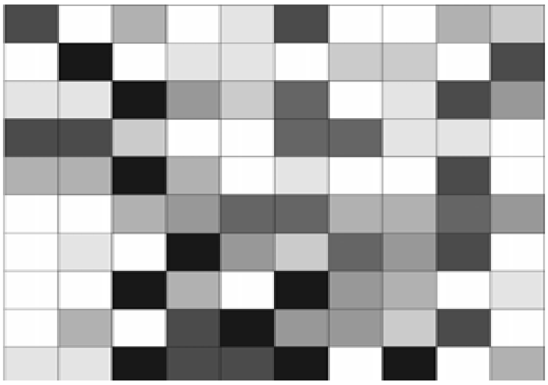


Fig4.2.1. *reserving room*

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access tothe original image.

4.2. Data Embedding

In the data embedding phase, some parameters are embedded into a small number of encryptedPixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodate dating the additional data and the original data at the positions occupied by theParameters. The detailed procedure is as follows According to a data-hiding key, the data-hider randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding. Here, Np is a small positive integer, for example, Np=20. The other (N-Np) encrypted pixels arePermuted and divided into a number of groups, each of which contains L pixels. The permutationWay is also determined by the data-hiding key. For each pixel-group, collect the M leastSignificant bits of the L pixels, and denote them as B (k,1) , B (k,2) …… B(k,M*L) where k is aGroup index within [1,(N-Np)/L] and M is a positive integer less than 5.The data-hider alsoGenerates a matrix G , which is composed of two parts. The left part is the identity matrix andThe right part is pseudo-random binary matrix derived from the data-hiding key.

4.3. Least Significant Bit (LSB)

Least significant bit (LSB) insertion is a common, simple approach to embeddingInformation in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can beUsed, since they are each represented by a byte. In other words, one can store 3 bits in

An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be As follows:

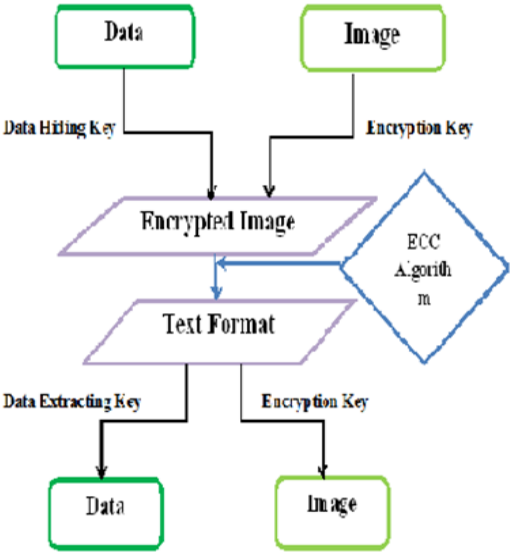
1. (00101101 00011100 11011100)
2. (10100110 11000100 00001100)
3. (11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into theleast significant bits of this part of the image, the resulting grid is as follows:

1. (00101101 00011101 11011100)
2. (10100110 11000101 00001100)
3. (11010010 10101100 01100011)

5. FLOW CHART

This flow chart represents the working of data hiding technique in encrypted images and converting it into text format by using ECC algorithm and by decrypting that text the original image and the hidden data can be regained.



6. ALGORITHM(ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite field. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S.Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.

For elliptic-curve-based protocols, it is assumed that finding the discrete algorithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key (see key size below).For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b, \tag{6.1}$$

along with a distinguished point at infinity denoted ∞.

The U.S. National Institute of Standards and Technology (NIST) have endorsed ECC in its suite B set of recommended algorithms, specifically Elliptic Curve Diffie-Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature. The U.S. National Security Agency (NSA) allows their use for protecting information classified up to top secret with 384-bit keys.

6.1. Text Formate

Preventing unauthorized access to corporate information system is essential for many organizations. Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure web browsing and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of this features. By using this algorithm the image is converted into a text format. And this text is send to the receiver. ECC provides a great security and more efficient performance than the first generation public key.

Soft-copy text is in many ways the most difficult place to hide data. This is due largely to the relative lack of redundant information in a text file as compared with a picture or a sound bite. While it is often possible to make imperceptible modifications to a picture, even an extra letter or period in text may be noticed by a casual reader. Data hiding in text is an exercise in the discovery of modifications that are not noticed by readers. Data hidden in text has a variety of applications, including copyright verification, authentication, and annotation.

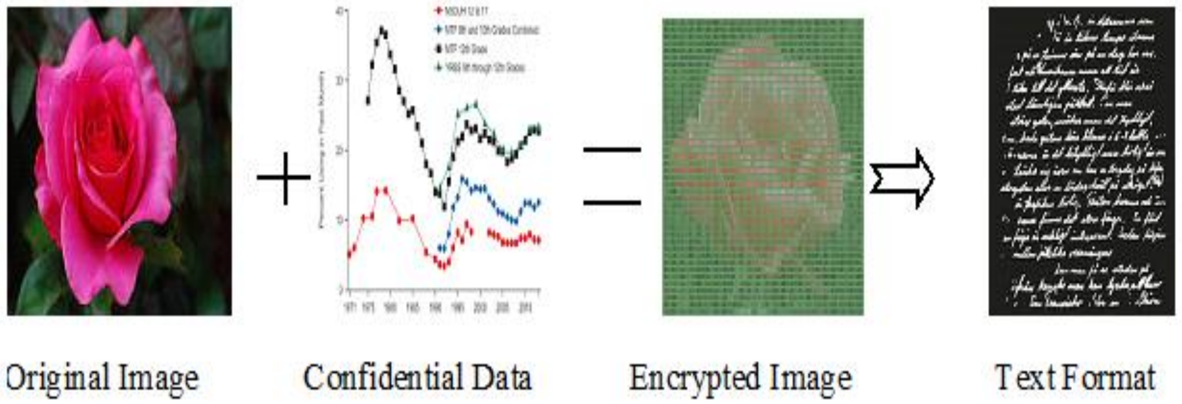


Fig6.1. *Overall Output*

7. ADVANTAGES

In our proposed system we have overcome the problems of existing system and the advantages of this are as follows:

- Ease of implementation: The portion between max and zero points in the histogram is intentionally shifted to the right by one. No calculation for performing this procedure is necessary.
- Guaranteed imperceptibility: The mean squared error (MSE) between the original and output images would be at most 1.00, meaning that the Peak Signal-to-Noise Ratio (PSNR) would be at least 48.13 dB.
- Little overhead: Only the luminance values of the max and zero points are required at the decoder for extracting the data and the original, meaning those 2 bytes (or 16 bits) of overhead is necessary, regardless of the size of original images.
- From the observations above, we are able to take the characteristics of the original image into consideration, and try to increase the capacity at the expense of somewhat degraded quality of the output image. Side information should be comparable to that of the conventional scheme. Therefore, we employ the concept of quad tree decomposition for the implementation of histogram-based reversible data hiding algorithm.

8. CONCLUSION

Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain animage similar to the original one using only the encryption key. When the receiver has both of The keys, he can extract the additional data and recover the original content without any error by Exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since

The lossless compression does not change the content of the encrypted image containingembedded data. However, the lossy compression method in compatible with encrypted images Generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation.Thus we are providing the double security to the confidential data by applying ECC algorithm and stenography. And it has a vast use in the future. Data hidden in text has a variety of applications, including copyright verification, authentication, and annotation. Making copyright information inseparable from the text is one way for publishers to protect their products in an era of increasing electronic distribution.

REFERENCES

[1] Besteena K.J, Philumon Joseph, Secure Reversible Data Hiding in Encrypted Images By Reserving Space In Advance, Volume-1, Issue-6, July 2014 ISSN 2348-6848

[2] Shilpa Sreekumar1, Vincy Salam2 Advanced Reversible Data Hiding With Encrypted Data Volume 13 Number 7-JUL 2014

[3] Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade Hide Inside-Separable Reversible Data Hiding in Encrypted Image, ISSN: 2278-3075, Volume-3, Issue-9, February 2014

[4] Xinpeng Zhang, Member, IEEE, Guorui Feng, Yanli Ren, and Zhenxing Qian, Scalable Coding of Encrypted Images, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 6, JUNE 2012

[5] Harshitha K M, Dr. P. A. Vijaya,Secure Data Hiding Algorithm Using Encrypted Secret message, International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.

[6] Harish G, Smitha Shekar B, Prajwal R, Sunil S Shetty, Reversible Data Hiding In Encrypted Images by Reserving Room before Encryption, International Journal of Engineering Research Volume No.3, Issue No.7, 01 July 2014

[7] Mr. Vikas Tyagi, Data Hiding in Image using least significant bit with cryptography , Volume 2, Issue 4, April 2012 .

[8] Minya Chen*, Edward K. Wong*, Nasir Memon* and Scott Adams+ Recent Developments in Document Image Watermarking and Data Hiding +Air Force Research Laboratory 32 Brooks Rd, Rome, NY 13441

[9] Deepthi C.Highly Secured Reversible Data Hiding in AES Encrypted Images by Reserving Room before Encryption with AuthenticationIJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014.