International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

An Approach for Security of Text by Steganography

[1]Suryabrata Das and [2]Prof. Samir Kumar Bandyopadhyay
[1]*B.S.C student, Department of Computer Science*
Ramakrishna Mission Vivekananda Centenary College, Rahara, India
[2]*GLA University, UP, India*

Date of Submission: 16-06-2020 Date of Acceptance: 02-07-2020

ABSTRACT
As an individual in the information society, information has been deeply integrated intothe individuals in society and has become an important organic part of individuals inmodern society. Therefore, the individuals in modern society should be called 'informationindividuals'. Seeing from this perspective, information security is also related to thepersonal and property security of 'information individuals' in modern society. Hence,protecting sensitive information is conducive to protecting the comprehensive securityof social 'information individuals' in the information age, which makes informationsecurity much more important in the contemporary era. In short, information security isa core and important issue that is of great concern to all of society today. In recent years, enormous research efforts have been utilized in the improvement of digital image steganographic techniques. The major aim of the paper is to use steganography for secure communication mechanism by embedding secret messages into digital images by modifying the nonessential pixels of the images.

KEYWORDS-Steganography, Cryptography, Compression, Least-Significant-Bit (LSB) Method, Stego-Image, and Cover-Image.

I. INTRODUCTION
Sensitive information security involves various technology and theories, and there aremany ways to achieve it. Embedding sensitive information into normal carriers(Steganography) to achieve safe transmission and protection of information is an effectivemethod of information security protection, which has been widely concerned andbecome a research hotspot in the field. Since text is the most widely used carrier ofinformation exchange, text-based steganography of personal information has importantresearch value and practical significance. Among the researches of text-based steganography,synonym replacement is the most typical scenario.Depending on the security level of the application thecomplexity of the program will be more complex structure,one who can optimize to use one or more of these individualfeatures. In this paper, we investigate the hand area, fingerarea and relative area based unique personalattribute and the angle between two fingers based on thelength of them for the recognition of hands. We apply imageenhancement, an edge detection technique, removal of someregion and then we apply our finial relative area-basedapproach with hand finger area calculations and determinationof angles. Hand geometry recognition systems may provide

three kinds of services verification, classification andidentification. For verification (hand geometry and the systemverifies her identity along with the user identity, forclassification known legitimate but does not supply anyidentity information of the user, for identification the userdoes not supply any identity information other than the hand-based geometry and may be an intruder. The system tries toidentify the individual or deny access. Therefore, we seen thatverification based on relative hand area may be a smartsubstitution due to its unobtrusiveness, low-cost and easyinterface, and low data storage requirements and thesesystems have gained immense popularity and publicacceptance as evident from their extensive deployment forapplications in access control, attendance tracking and severalother verification tasks.

II. REVIEW WORKS
After the embedding of the secret message these images are called as stego-image and it is used to communicate through a public channel [1-2]. Used public channel may be intentionally monitored by some opponent in the transmission process, who tries to prevent successfully communications and he/she may randomly attack few stego-images in case of doubt on stego-images [3]. High imperceptibility (similarities between the cover-image and the stego-image) is the only way to reduce the chances of doubt on stego-images and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

increases the chances of secure communications [4]. An alternative was proposed by [5], it make use of a stego key to provide additional security on the secret data.

In past few decades, many steganographic techniques were proposed for still images, one of them is a simple and well- known approach is directly hiding secret data into the least-significant bit (LSB) of each pixel of an image. JarnoMielikainen [6] proposed its improved version to improve imperceptibility, it allows the embedding of the same amount of secret data with fewer changes to the cover-image, it makes the detection harder as comparison of conventional LSB matching method. [7] Proposed a statistical method for detection in LSB technique. Although it is susceptible to noise over the network but it is useful for sensitive and valuable information like Pan Card details, Form16 etc., on a system which is accessible to many of them. The LSB-based methods mentioned above are embedding the secret messages directly into the spatial domain in an unreasonable way without taking into consideration of the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is always higher than a smooth area [8]. A generative model for recognitions of hand and total pixels calculations principal to along-likelihood objective function which aims to enclosehand-like pixels within the projected silhouette of the three-dimensional model while excluding backgroundlike pixels.Segmentation and hand-pose estimation are jointly addressedthrough the minimization of a single likelihood function [2].Pose is determined through gradient drops in the hand edges(both left and right pixels) of such an area-based objectivefunction. Pointing Based Object Localization [3]computationally feasible, recognize the object. Currently, most steganographic methods aim to defininga better distortion function [5] or improving it [6]to achieve high un-detectability. However, these modificationsmadeby steganography provide possibilitiesfor steganalysis. Many steganalytic methods havebeen developed to defeat steganography. Feature extractionand machine learning-based steganalysis has beenproved to be efficient [7]. A variety of feature extraction

algorithms have been proposed [8,9]. Meanwhile,the ensemble classifier [10] is widely used to measurethe feature sets. Recently, deep learning-based steganalysis[6-7] has achieved good performance, whichcan disclose the existence of covert communicationwith a high probability even when low payload is carried.Therefore, new approaches of steganography aredesirable.Different from traditional steganography which transmitssecret data by modifying the content of multimedia[10], behavioral steganography hides secret data intonormal behaviors in social networks. For example, in[8], the length of a tweet is modulated to carry data.In [5], the secret data is carried by directly retweetingor tweeting by simply quoting the retweeted account's tweet. These methods are simple attempts of behavioralsteganography.

Proposed Method

Communication is a very important word with respect to civilization. Nations who cannot communicate with other basically lost their identity. With the advancement of technology today communications are mostly done through internet which is open and public in nature. So, information protection has become most vital issue and ongoing topic of research. During the transformation if information is intentionally or unintentionally modified it lost its meaning. The information may be protected against these adversaries if we can hide the existence of the message [1].

Steganography can be an effective for this secure communication through these digital media. Its aim is to hide the very existence of the message in the cover medium [2]. The term steganography was only coined at the end of the 15th century but data hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves are the early use of it [3]. Recently at the time of World War II people also use invisible writing by the help of invisible ink. Modern steganography is generally understood to deal with electronic media rather than physical objects. Steganography is the combination of two Greek words "stegos" (means "cover") and "grafia" (means) "writing" defining it as "covered writing" [4, 10]. The basic requirements of Steganography are:

Cover media that can hold the hidden information.

• The secret message (target message) that basically embed within the cover media.

• A steganography function and its inverse.

Based on the different media we have text, image, audio, video and protocol Steganography where the cover medium are text, image, audio, video, and IP packet respectively [5]. Both the spatial and transform domain embedding scheme as well as for each of the cover media has to maintain the challenges of Steganography which are imperceptibility, robustness and capacity.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

Imperceptibility is concerned with the fact that human being should not become suspicious of the existence of the covert data within the medium. Robustness ensures that once a secret message is inserted, it becomes impossible to delete or manipulate that message. Moreover, the capacity of the digital media deals with the fact that how much target we can embed within the cover file without less distortion of it [6]. But these factors are depend on each other and a balance must be maintained between them as increase in one of the factors leads to the decrease in other.

Following are the domains in which steganography techniques are divided:

a) Frequency Domain Technique: In this technique use of various algorithms and modifications are done to hide information, it a zone of embedded methods on which number of algorithms is suggested, this technique is a bit tedious and is classified as follows:

- Discrete cosine transformation technique: For the conversion of a signal into elementary frequency components discrete cosine transform (DCT) is used.
- Discrete Wavelet transformation technique: When the wavelets are discretely sampled, it is a discrete wavelet transform (DWT).
- Discrete Fourier transformation technique: The use of this technique is done to get frequency component of every pixel value.

b) Spatial Domain Methods: In this method few bits of image pixel are directly changed in order to hide data. This technique is classified as follows:

- Pixel value differencing: In this technique a quantization range table is designed,payload is determined and maintenance of the countability of steganography is done.
- Edge based data embedding method: In this method, in an image every edge pixel is used. Firstly we calculate the masked image and identify edge pixels through canny edge detection method. In LSB bits of the edge pixel the data is hidden and receiver receives the steganographic object.
- Least significant Bit:In a string LSB is the lowest bit, it is the rightmost key in thestring, example, in the binary number: 110100101001, the far right 1 is LSB. In LSB of image, secret information is stored.
- Random pixel embedding method: This method is employed to implant and transmit steganography object.

LSB technique Benefits:

1. Quality of main image is maintained.
2. Enhancement in capacity for information storage.

LSB technique disadvantages:

1. Low strength, image data might get lost.
2. Attacks can easily destroy hidden data

In our proposed method we try to we concentrate on how much target data we can embed into the cover file so that human sense cannot follow its existence. Here a binary image is hidden within another which is basically a colour image. And we also try to increase the robustness of stego image by increasing the depth of LSB layer. Basically image Steganography technique try to hide the existence of the so that it can cheat the HVS [7-8].

As target data we consider a very important biometric authentication data – signature. In our proposed technique we consider that the signature image is basically a binary image and we try to hide this binary image within a 24-bit Color image. In case of a binary image each pixel is 1 bit long and can have values as either 0 or 1, whereas in case of a color image, each pixel is 24 bit long. These 24 bits can be thought of as a collection of 3 bytes where the first byte (first 8 bits) signify the intensity of red component, the next byte signifies green component and the last byte signify blue component.

In our method first we have replaced the 5th bit (from the LSB) of each of the R, G and B component of the cover image with the pixel value of the target image, which is either 0 or 1. if I want to store 1 in a binary string S='11101011'(235), then S(5)=0 is replaced by 1 and if I want to store 0 in a binary string S='10111111' (191), then S(5)=1 is replaced by 0. Thus the modified string becomes S='11111011' (251) and S= '10101111' (175) respectively. In both cases the difference between original and modified pixel value is 16. So replacing the 5th bit may give rise to a problem. From the example stated above it is observed that a changing only in the 5th bit can change the entire value of the string up to a maximum of 16. In our proposed technique we try to adjust the bits of the original string after embedding the data in the 5th LSB layer to reduce this difference [9].

Technique for bit adjustment to minimize the change in pixel value due to replacement of 5th LSB layer we consider 3 possible cases.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

Case 1: 5th bit changes from 1 to 0
Again it has 4 sub cases:

Table 1(a)

Sub-case no.	Specifications	Action taken
1.1	when the 4th and 6th bit (from LSB) are 0 and 0 respectively	Set all the bits to the right of the 5th bit (i.e., towards LSB) to 1.
1.2	when the 4th and 6th bit (from LSB) are 0 and 1 respectively	Set all the bits to the right of the 5th bit (i.e., towards LSB) to 1
1.3	when the 4th and 6th bit (from LSB) are 1 and 0 respectively	Set all the bits to the right of the 5th bit (i.e., towards LSB) to 0 and set the 6th bit (first bit to the left of the 5th bit) to 1.
1.4	When the 4th and 6th bit are 1 and 1 respectively.	Set all the bits to the right of the 5th bit (i.e., towards LSB) to 0 and set all the bits to the left of the 5th bit (i.e., towards the MSB) to 0 until a 0 is encountered. When a 0 is encountered, set it to 1.

Case 2: 3rd bit changes from 0 to 1.
Again it also has 4 sub cases

Table 1(b)

Sub-case no.	Specifications	Action taken
2.1	when the 4th and 6th bit are 1 and 1 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 0.
2.2	when the 4th and 6th bit are 1 and 0 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 0
2.3	when the 4th and 6th bit are 0 and 1 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 1 and set the 6th bit(first bit to the left of the 5th bit) to 0
2.4	when the 4th and 6th bit are 0 and 0 (from LSB) respectively	Set all the bits to the right of the 5th bit (i.e towards LSB) to 1 and set all the bits to the left of the 5th bit (i.e towards the MSB) to 1 until a 1 is encountered. When a 1 is encountered, set it to 0.

Case 3: No change at all. If the bit which I want to place at the 3rd LSB position of the pixel value is same with the 3rd LSB of the original pixel value then the original pixel value become unchanged. Here I also may think of two sub-cases: 0 and replace with 0 and 1 and replace with 1.
Now we demonstrate the first two cases and their sub cases of our proposed method with some examples.
Case 1: 5th bit changes from 1 to 0
Case 2: 5th bit changes from 0 to 1

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

Case 1.1:

when the 4th and 6th bit (from LSB) are 0 and 0 respectively		8	7	6	5	4	3	2	1
Original intensity value	146	1	0	0	1	0	0	1	0
After Replacement of 5th bit with 0	130	1	0	0	0	0	0	1	0
Modified intensity value with shaded bits	143	1	0	0	0	1	1	1	1

Case 1.2:

when the 4th and 6th bit (from LSB) are 0 and 1 respectively		8	7	6	5	4	3	2	1
Original intensity value	178	1	0	1	1	0	0	1	0
After Replacement of 5th bit with 0	162	1	0	1	0	0	0	1	0
Modified intensity value with shaded bits	175	1	0	1	0	1	1	1	1

Case 1.3:

when the 4th and 6th bit (from LSB) are 1 and 0 respectively		8	7	6	5	4	3	2	1
Original intensity value	154	1	0	0	1	1	0	1	0
After Replacement of 5th bit with 0	138	1	0	0	0	1	0	1	0
Modified intensity value with shaded bits	160	1	0	1	0	0	0	0	0

Case 1.4:

When the 4th and 6th bit are 1 and 1 respectively		8	7	6	5	4	3	2	1
Original intensity value	186	1	0	1	1	1	0	1	0
After Replacement of 5th bit with 0	170	1	0	1	0	1	0	1	0
Modified intensity value with shaded bits	192	1	1	0	0	0	0	0	0

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

Case 2.1:

when the 4th and 6th bit are 1 and 1 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	170	1	0	1	0	1	0	1	0
After Replacement of 5th bit with 0	186	1	0	1	1	1	0	1	0
Modified intensity value with shaded bits	176	1	0	1	1	0	0	0	0

Case 2.2:

when the 4th and 6th bit are 1 and 0 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	138	1	0	0	0	1	0	1	0
After Replacement of 5th bit with 0	154	1	0	0	1	1	0	1	0
Modified intensity value with shaded bits	144	1	0	0	1	0	0	0	0

Case 2.3:

when the 4th and 6th bit are 0 and 1 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	162	1	0	1	0	0	0	1	0
After Replacement of 5th bit with 0	178	1	0	1	1	0	0	1	0
Modified intensity value with shaded bits	159	1	0	0	1	1	1	1	1

Case 2.4:

when the 4th and 6th bit are 0 and 0 (from LSB) respectively		8	7	6	5	4	3	2	1
Original intensity value	130	1	0	0	0	0	0	1	0
After Replacement of 5th bit with 0	146	1	0	0	1	0	0	1	0
Modified intensity value with shaded bits	127	0	1	1	1	1	1	1	1

We can see from the above example that the maximum change in the modified pixel is 8 instead of 16. After the adjustment of the bits due to enhancement of perceptual transparency we

replace LSB (1st bit) for increasing the capacity of the stego file and for this case the max change is 9.

In case of binary image each pixel can have only 2 values, either 0 or 1. Thus when I apply this algorithm to hide a binary image within a 24 bit RGB image, I can embed 2 pixels of the target image in each of the R, G and B component of the cover image- one in the 5th LSB and another in the 1st LSB position. Thus a total of 6 pixels of the target image can be stored in one pixel of the cover image.

Since 6 pixel of the target image can be saved in 1 pixel of the cover image, instead of embedding the target pixels in consecutive pixels of the cover image from the 2nd row. For hiding the data we do not consider the consecutive pixel we choose the pixels one after the other.

The first row is used for embedding image size. We store this value based on digits of row and column value. Now we explain this by an example let the binary image size be 87×123. So row value is 87 and column value is 123. The number of digits in row value is 2 in binary it is 0010 and stores it in 1st and 2nd LSB of R and G plane of 1st pixel. The corresponding number of digits in column size is stored in 1st and 2nd LSB of R and G plane of 2nd pixel.. Then the individual digits (like 8,7,1,2,3) of row and column size are stored in consecutive 1st and 2nd LSB of R and G plane pixel of first row starting from 5th pixel, row and then column basis.

At the receiver side we first collect the size of the target image and then try to form the target image by extracting data from it. Here we take a pixel of stego image and pick the 5th and 1st LSB of each of the three planes R, G and B. These six bits form six pixels of target signature image. Like this the other pixels of target image are formed.

Here in this method we consider 5th LSB for inserting data one target data. By increasing the depth of LSB layer we try to remove the main disadvantage of standard LSB coding techniques which is low robustness. But when we increase the depth of LSB layer during LSB coding the probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. In our proposed method we try to minimize this limitation by using an adjustment technique. Without applying this adjustment technique if we embed a target data at 5th LSB position the modified pixel's intensity value become 16 more than the original (24). But in our proposed technique it reduces to at most 8.

Then we embed next target data at LSB for increasing the capacity of the stego image and for this the difference between original and modified pixel's intensity value becomes at most 9.

Since 6 pixels of target image is hidden in one pixel of RGB colour image so I can hide a binary image of size 5 times more than the cover image into that particular cover image. By this we can meet one of the challenges of Steganography.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 488-496www.ijaem.net ISSN: 2395-5252

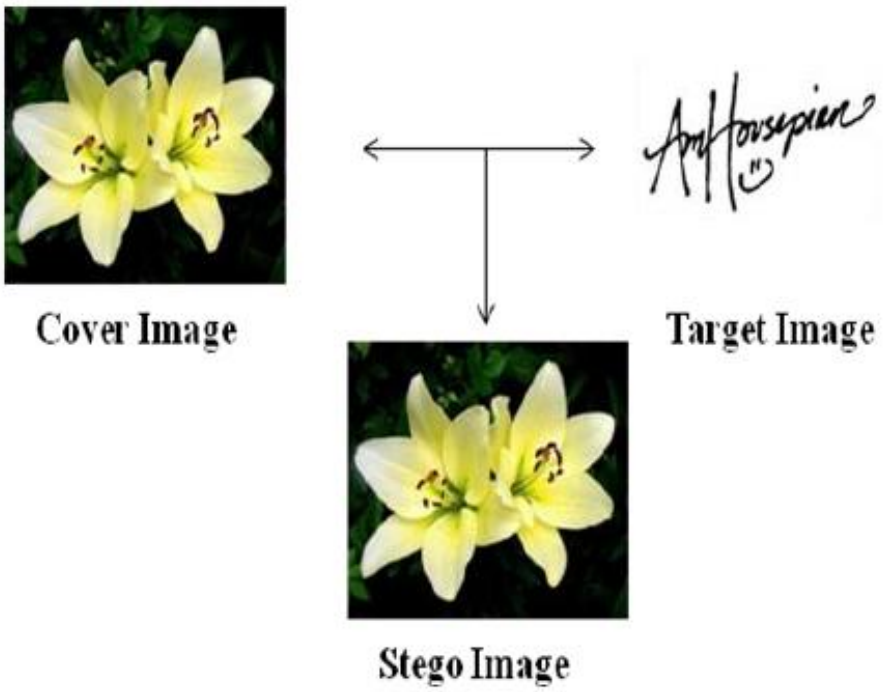

Figure 1. Test Case 1

Figure 2. Test Case 2

III. CONCLUSIONS

In this modern era where security becomes an important issue, Steganography plays a vital role for secure communication. Authentication, data integrity as well as confidentiality issues are maintained in our work because we hide the signature of a person within an image in such a way so that no one can understand its existence. In our proposed method we meet the three challenges of Steganography mainly capacity by hiding a binary image within an RGB image.

REFERENCES

[1]. M. Kharrazi, H. T. Sencar and N. Memon, "Image Steganography: Concepts and Practice", Lecture Notes Series", Institute for Mathematical Sciences, National University of Singapore, Singapore, (2004).
[2]. B. Pfitzmann, "Information Hiding Terminology", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, (1996) May 30-June1, Lecture notes in Computer Science, vol. 1174, Ross Anderson (Ed.), pp. 347-350.
[3]. J. Fridich and R. Du, "Secure Steganographics Methods for Palette Images", In Information Hiding, 3rd International Workshop, Springer, (1999), pp. 47-60.
[4]. N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer, vol. 31, no. 2, (1998), pp. 26–34.
[5]. R. B. Wolfgang and E. J. Delp, "Watermark for digital images", Proceeding of the IEEE International Conference on Image Processing, IEEE Computer Society, Washington DC, USA, (1996) September 16-19, pp. 219-222.
[6]. C. C. Chang, T. D. Kieu and Y. C. Chou, "High capacity data hiding for grayscale images", In Proceedings of the First International Conference on Ubiquitous Information Management and Communication, Seoul, Korea, (2007) February, pp. 139–148.
[7]. C. Parthasarathy and S. K. Srivatsa, "Increased Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding", Journal of Theoretical and Applied Information Technology, vol. 7, (2005 – 2009), pp. 080 - 086.
[8]. S. K. Bandyopadhay, B. Datta and K. Dutta, "Information Hiding in Higher LSB Layer in an Audio Image", International Journal of Advanced Research in Computer Science, vol. 2, no. 3, (2011).
[9]. S. K. Bandyopadhay and B. Datta, "Higher LSB Layer Based Audio Steganography Technique", International Journal on Electronics & Communication Technology, vol. 2, Issue 4, (2011) October - December, pp. 129-135.
[10]. G. Paul, I. Davidson, I. Mukherjee and S. S. Ravi, "Keyless Steganography in Spatial Domain using Energetic Pixels", In Proceedings of the 8th International Conference on Information Systems Security (ICISS), (2012) December 15-19, Guwahati, India, vol. 7671, LNCS, Springer, pp. 134-148.