INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING TECHNOLOGY AND APPLIED SCIENCES (IJIETAS)

ENCODING AND DECODING HIDDEN MESSAGES IN IMAGES USING STEGANOGRAPHY

[1]Sushmita, [2]Mir Rimsha, [3]Ali Murtaza Zaidi

[1]Sharda University Greater Noida, Sushmitaa.sv@gmail.com
[2]SET, Sharda UniversityGreater Noida,2020459147, mir@ug.sharda.ac.in
[3]Sharda University Greater Noida 2020497849, ali@ug.sharda.ac.in

ABSTRACT

Visual Cryptography is a technique to share secret code in the form of images. Steganography is usedto encrypt these images into hidden codes which in earlier times is used as a mode of communication in the time of war. These hidden codes have their way of decryption, sharing images multiple times can decrypt these images. The encryption in these images is done in pixels so that it won't be visible to the naked eye. The small changes in these images can be only visible by superimposing. After superimposing we can not recoverthe original image because of contrast and expansion in pixels of the image. The visual form of steganography is the safest form that is present nowadays. In this paper, we will know how we can encrypt this image in hidden form using cipher text and steganography and prevent itfrom being disposed of by the naked eye.

Keywords: Cryptography, Steganography, Cipher, Hidden Image, Visual Cryptography, Encryption, Decryption, Asymmetric key, Symmetric key..

DOI:

1 Introduction

In today's world, huge types of cryptographic models have been introduced to date. The cryptography system's primary goal model is to convert the main message into a hidden code so that the secret message only stays between the sender and receiver. In cryptography, we use ciphers to convert our message into hidden code. There are several methods from which we can hide our message but, in this paper, we are using the steganography technique to hide our secret code inan image.

Steganography is a famous technique that has been used since 440 B.C. to hide messages in the form of invisible ink and in modern times this method is used in articles and papers. Visual Steganography has been in use since 1985, with the improvement and evolution in the computer system, techniques of steganography have also evolved. Visual Steganography is usually used in media folders like jpeg. &png. Images. The encoding in these images is done in pixels as jpeg and png images do not show much distortion because of their wide color spectrum and due to this hiding codes andsecret messages in this message becomes easy.

Various types of algorithms can help in implementingsteganography in visual media:

- Embedding Using the Least Significant Bit (LSB)
- Techniques for Masking and Filtering
- Encoding with Redundant Patterns
- Encryption and Randomized Distribution

➢ **The insertion of the least significant bit (LSB)** the most famous algorithm in steganography for images. Inthis, the hidden codes are stored in pixels and it does not show any changes after and before the alteration in the image. In this, the image is hiddenin the noise level.

➢ To work with 24-bit, grey-**scale images masking techniques** are the best. It is also used as a watermark to hide the hidden code in other wordsmasking the secret code. Changes in multiple proportions are necessary for this to make sure thatthe hidden message cannot be detected. This technique is stronger than the LSB technique as ithides the message in the inner parts of images.

- **Redundant Pattern Encoding** is the same as the spectrum technique. After using this technique, we cannot crop or rotate the image so it becomes easy for others to identify whether the image has any hidden code or not. In this, the message is dispersed in all the parts of the image.

- **Encrypt and scatter technique** is the same as theRedundant Pattern Technique as in this algorithm images are distributed in the different parts of image pixels. This message is converted into numbers these numbers are dispersed in the different parts of the image. This technique is saferthan LSB as decoding the numbers bit by bit is tuff.

Proposed Method

Visual data stored in picture frames are usually known asimages. These images are made up of pixels and these pixels
are made of three colors that are red, blue, and green. We manipulate these colors and hide data in them to hide the secret message. By doing this the image will only differ withslight changes in color. These colors can also act as a hideoutfor the data we are trying to keep secret.
To ensure that the level of protection is high, the Reference of the algorithm is used here as shown in the fig1. Various reference grid is used in this reference database. The character encoding scheme that will be applied in terms of certain integers will be shown in three dimensions on each of these grids. (A different character ona different grid may or may not be represented by the same number.

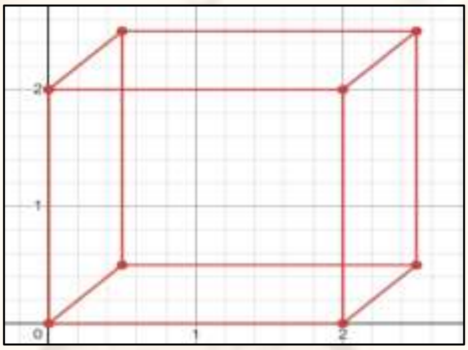

Fig1. Reference database

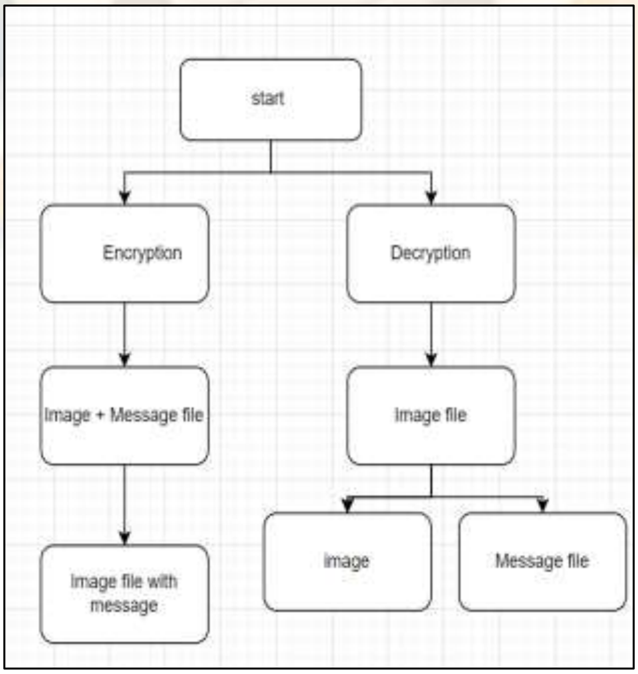

Fig. 2. Flowchart of encoding and decoding of secret code

1. Encryption Algorithm

1. Convert each character of the data into its corresponding ASCII value and represent it as an 8- bit binary sequence
2. Total of 3*3=9 RGB values in the three pixelsthat are read at once.
3. 8-bit binary character is stored using the first eightRGB values.
4. The binary data and its related RGB values are contrasted. The RGB value is converted into odd if the binary digit is 1,and into even otherwise.
5. Use the ninth RGB value as a control flag: set it to even if there is more information to process or encode, and to odd if there is no further data to read or embed.
6. The process will continue until data is encrypted into theimage.

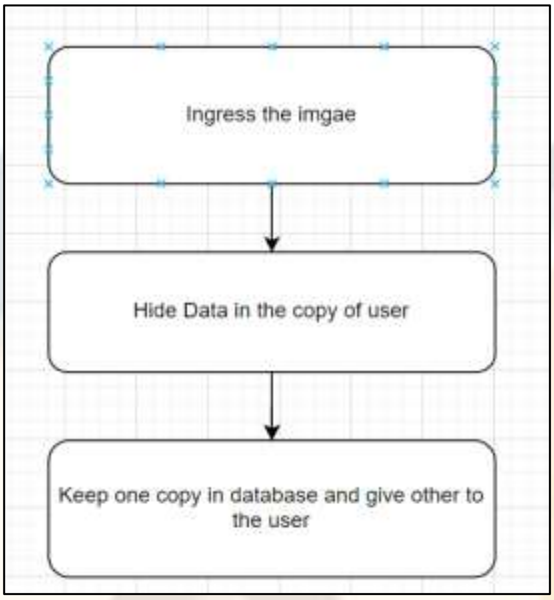

Fig 3. Flowchart of encrypting the secret code.

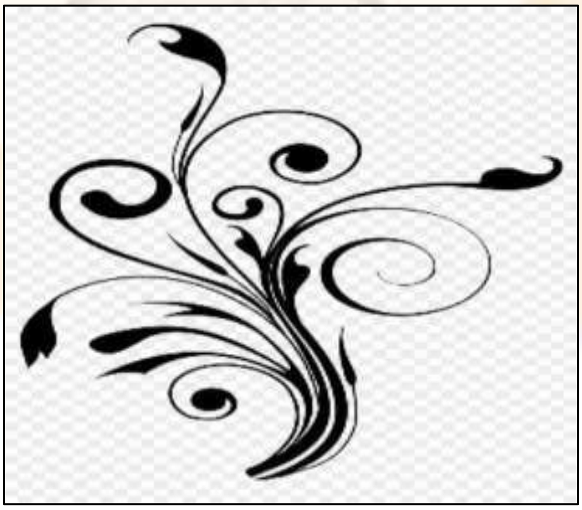

Fig 4. Image before Encryption

2. Decryption Algorithm

1. Three pixels values are read at a time. The first eight RGB values inform us of the secret data, and the ninth value indicates if we should proceed or not.
2. For the first eight numbers, the binary bit is 1 for oddvalues otherwise it is 0.
3. The bits are combined to form a string, and everythree pixels, or one character, corresponds to a byte of secret data.
4. If the ninth value is even, we shall continue reading threepixels at a time, it concludes that there is no hidden information present in those pixels.

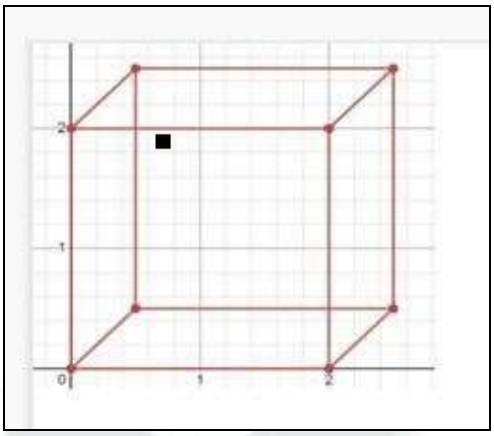

Fig5. Encoded image reference database

Fig 6. Encoded Image

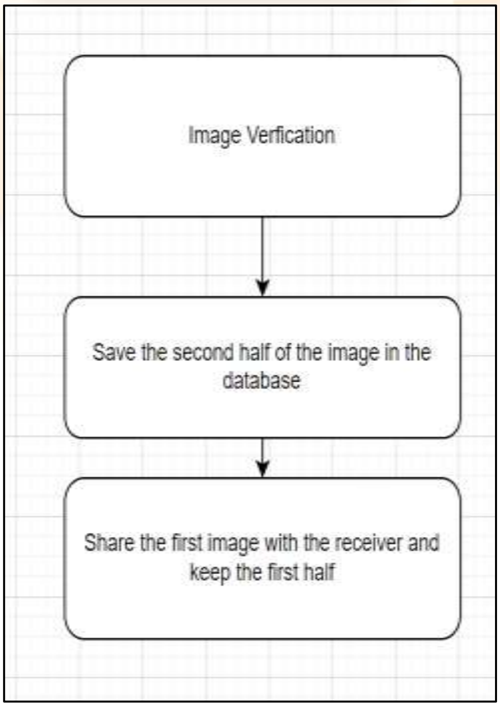

Fig. 7. Encoding secret code.

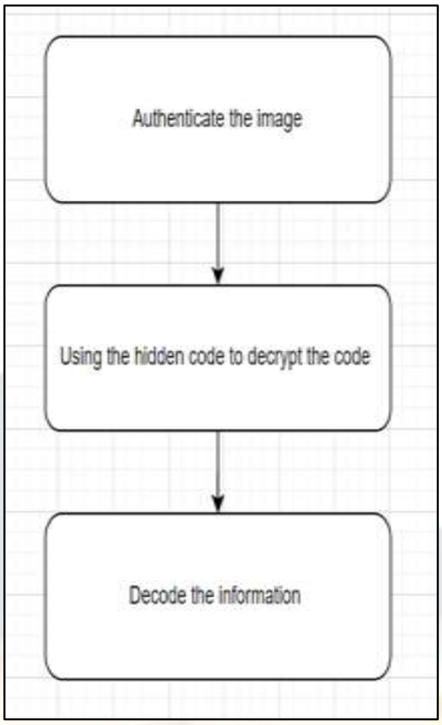

Fig 8. Decoding secret code

Result And Discussion

The system was created using a 200x150 (30000) pixel picture. The pixel values were initially raised to the following larger multiple of 5. The DEA algorithm was usedto transform the message text into cipher text. 'This is the Secret Key' served as the secret key. One byte per pixel wasused when calculating the maximum size for the message data (29 Kb). Then, Using the pixel variation (decrement) of the selected value, which ranged from 0 to 4 for the pixel's R, G, and B values, cipher text was embedded into the jpeg picture. There were three data grids in the reference database. The image's pixel count served as the foundation for choosing the data grid. Data grid 1 waschosen if there were data grid 2, and if there were fewer than one million pixels, if there were between one million and ten million pixels. 3 if there were more than 1,00,000 pixels. There were 20 matrices total in each data grid, and they were chosen based on their height-to-width ratio. No discernible distortion was discovered in the picture of the message data.

By examining pixel changes, the cipher was located for decryption, and the message was located using the inverse DEA function. Pixels' density difference from the subsequent higher multiple of 5 was computed in order to extract the cipher from the picture. the size of the image's pixels served as the foundation for choosing the appropriate data grid from the reference database. The height- to-width ratio was used to choose the appropriate matrix the information grid. The secured message was then extracted from the picture after that. This communication was encrypted, and the original message text was recoveredusing the inverse DEA function.

Future Work

Images of any size might be incorporated into the system through modification. The output might be improved. The system might be strengthened by integrating the model with another authentication method, such as biometric authentication. The concept might also be modified to work effectively with certain hardware, such as different cell phones. The only permissions available in the model right now are Read and Write. It might be improved much furtherby adding rights like Modify and Delete. The top access level, which is often the administrator level, might have twolevels of protection.

References

1. R. S. Sandhu and P. Samarati, "Access control: principleand practice," IEEE
2. M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryp — EUROCRYPT'94. Springer Berlin Heidelberg
3. N. F. Johnson and S. Jajodia, "Exploring steganography:Seeing the unseen,"
4. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Rolebased access control models," Computer,
5. M. Naor and B. Pinkas, "Visual authentication andidentification," in Advances in Cryptology — CRYPTO '97.
6. R. V.R., J. J., and J. M., "A visual cryptographic scheme for owner authentication using embedded shares," vol. 5, no.
7. M. B. Goel, V. B. Bhagat, and V. K. Katankar, "Authentication framework using visual cryptography," vol.2, no. 11, pp. 271–274, 2021.
8. Jaya, S. Malik, A. Aggarwal, and A. Sardana, "Novel authentication system using visual cryptography," in 2019 World Congress on Information and Communication Technologies, Dec 2011
9. C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, "Secure authentication using image processing and visual cryptography for banking applications," in 2008 16th International Conference on Advanced Computing and Communications, Dec 2018, pp. 65–72.
10. C.-N. Yang, L.-Z. Sun, X. Yan, and C. Kim, "Design anew visual cryptography for human- verifiable authentication in accessing a database," Journal of Real- Time Image Processing, vol. 12, no. 2, pp. 483–494, Aug 2019. [Online]. Available: https://doi.org/10.1007/s11554- 015-0511-9
11. . Falkner, P. Kieseberg, D. E. Simos, C. Traxler, and E.Weippl, "Evoting authentication with qr-codes," in Human Aspects of Information Security, Privacy, and Trust. Cham: Springer International Publishing, 2019, pp. 149–159.
12. P. Sanyasi Naidu and R. Kharat, "Multi-factor authentication using recursive xor-based visual cryptography in online voting system," in Security in Computing and Communications. Springer Singapore, 2018,pp. 52–62.
13. R. Ajjipura Basavegowda and S. Holalu Seenappa, "Secret code authentication using enhanced visualcryptography," in Emerging Research in Electronics
14. Mizuho NAKAJIMA, "Extended use of VisualCryptography for natural images, Department of Graphics and Computer Sciences", Graduate School of Arts and Sciences, The University of Tokyo
15. Bart Preneel, "Cryptographic Algorithms: Basicconcepts and application to multimedia security",Katholieke University, Belgium
16. Information Security", National Institute ofStandards and Technology, Special Publication, 2019.