RESEARCH ARTICLE

Separable Reversible Data Hiding in an Encrypted Image

Jaimini Solanki, Faizal Patel, Vivek Rajguru, Ankit Saxena
Medicaps Institute of Technology and Management,Indore, MP, India

Abstract: Since times immemorial, security of data to maintain its confidentiality, proper access control, integrity and availability has been a major issue in data communication. Today images and data transfer in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily lives. We wanted to develop a scheme in which the data embedded in an image and the image itself would be secured from any unauthorized access. This scheme would also be a merit in military and medical services. This paper proposed a scheme for separable reversible data hiding technique in an encrypted image. The original image was encrypted using an encryption key. Then, a data-hider hides the data using the data-hiding key. With an encrypted image containing additional data, if a receiver has the data-hiding key, it can extract the additional data though it does not know the image content and if it has the encryption key, it can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the key it can extract the additional data and recover the original content without any error by exploiting. This results in the security of data and image privacy.
Keywords: encryption decryption; hill cipher method; MATLAB; cryptography; data-hiding key; data embedding

1. Introduction

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data. There are two basic types of cryptography or encryption schemes: Symmetric-key and public-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus, communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention: historically, all encryption schemes have been symmetric-key (also called private-key) schemes. This paper focuses on separable reversible data hiding which will result in security of both the data and image independently.Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems.

For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and

doi: 10.18686/wct.v3i2.

protect software against reverse engineering (see also copy protection) is another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

1.1 Literature Review

In[1] authors described that reversible data hiding emphases on the data embedding/extracting on the plain spatial domain. But, in some scenarios, a media assistant or a channel administrator hopes to append some additional message, such as the origin, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content (payload) should be recovered without any error after image decryption and message extraction at receiver side. In[2] the authors presented that a content owner encrypts the original image using an encryption key, and a data-hide embeds additional data into the encrypted image using a data hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.

In[3] the scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data In[4] authors brings in account a new method for embedding the data inside the image using ordinal virtual embedding technique and along with modification of data, for the security of information.

In[5] authors proposed a discrete reversible data hiding in cipher images which deals with security and authentication. Firstly, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider is used to compress the least significant bits of the encrypted image using a data hiding key. If a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. And if the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract both, additional data and recover the original content. In[6] authors introduced an effective scheme of separable reversible data hiding for encrypted image using histogram modification. After the original image is encrypted by the sender, the data-hider embeds the secret message into the encrypted image using a histogram modification and n-nary data hiding scheme. On the receiver side, the secret message can be extracted by the embedding key. In[7] authors proposed a different methodology which attains real reversibility by reserving room before encryption with the RDH algorithm, and then encrypting the data and embedding the data in the encrypted image, which is encrypted by a new algorithm. The proposed method can achieve real reversibility that is data extraction and image recoveries are errorless.

1.2 Outline

In Section 2, we discussed the general system for Encryption and Decryption. In section III, the implementation of the Encryption and Decryption is described using Hill Cipher method. Section IV gives the results and observation followed by the Section V, which gives the conclusion of the paper along with its future scope.

1.3 Tools used

We used MATLAB R2010a as our platform to work on our paper. The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK papers, which together represent the state-of-the-art in software for matrix computation. MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis MATLAB is a high-performance language for tech-

nical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

2. Encryption/Decryption System

The flowchart of general system for Encryption and Decryption shown in **Figure 1**.

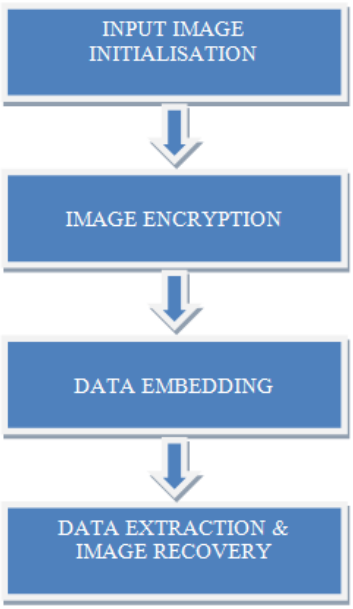
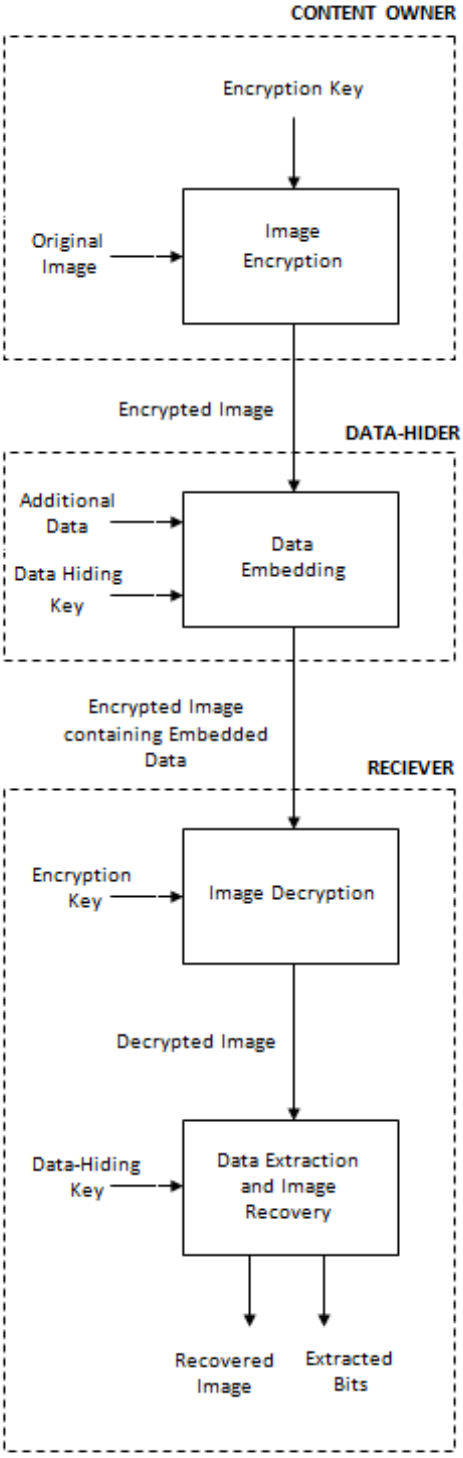


Figure 1; General system block diagram

There are two basic types of encryption schemes: Symmetric-key and public-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus, communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages.

However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention: historically, all encryption schemes have been symmetric-key (also called private-key) schemes. The block diagram for Non separable reversible data hiding in an encrypted image is shown in **Figure 2.**



S

Figure 2; Non separable reversible data hiding in an encrypted image.

3. Implementation Of Encryption and Decryption System

The flowchart for the implementation of Encryption and Decryption system is shown below in **Figure 3.**

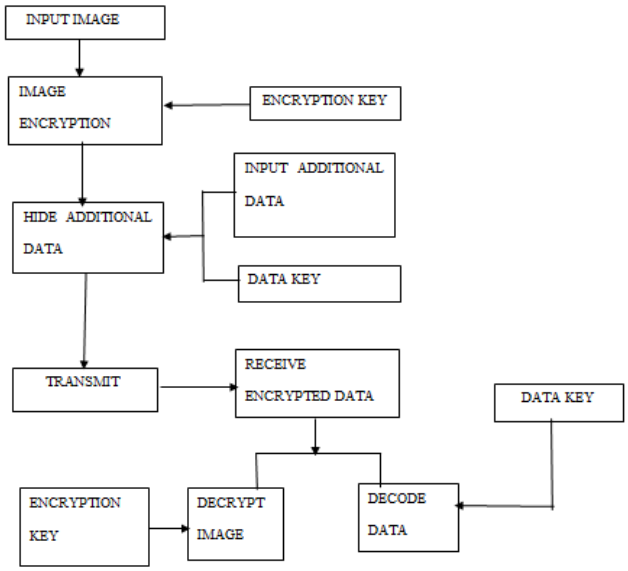


Figure 3; Separable reversible data hiding in an encrypted image.

3.1 Hill Cipher Method Implementaion

The core of Hill-cipher is matrix manipulations. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher each character is assigned a numerical value like: a=0, b=1, …….. z=25.

The substitution of cipher text letters in place of plain text leads to m linear equations. For m=3, the system can be described as follows:

$c_1 = |(k_{11}p_1 + k_{12}p_2 + {}_{13}p_3)|$

$c_1 = |(k_{21}p_1 + k_{22}p_2 + k_{23}p_3)|$

$c_1 = |(k_{31}p_1 + k_{32}p_2 + k_{33}p_3)|$

This can be expressed in terms of column vectors and matrices:

C=KP

Where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a 3*3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires the inverse of matrix K. The inverse K-1 of a matrix K is defined by the equation.

$k*p^{-1}$= I where I is the Identity matrix.

NOTE: The inverse of a matrix doesn't always exist, but when it does it satisfies the proceeding equation.

k^{-1} is applied to the cipher text, and then the plain text is recovered. In general terms we can write as follows:

For encryption: $C=D_k(P)=Kip$

For decryption: $P=E_k(C) =p^{-1}$ $C= k^{-1}Kp=P$

As we have seen in Hill cipher decryption, it requires the inverse of a matrix. So, while one problem arises that is: Inverse of the matrix doesn't always exist. Then if the matrix is not invertible then encrypted text cannot be decrypted. In order to overcome this problem author suggests the use of self-repetitive matrix. This matrix if multiplied with itself for a given mod value (i.e. mod value of the matrix is taken after every multiplication) will eventually result in an identity matrix after N multiplications. So, after N+ 1 multiplication the matrix will repeat itself. Hence, it derives its name i.e.self-repetitive matrix. It should be non-singular square matrix.

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector

$$\begin{matrix} 0 \\ 2 \\ 19 \end{matrix}$$

{\displaystyle {\begin{pmatrix}6&24&1\\13&16&10\\20&17&15\end{pmatrix}}}

Thus, the enciphered vector is given by:

$$\begin{matrix}6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15\end{matrix} * \begin{matrix}0 \\ 2 \\ 19\end{matrix} = \begin{matrix}67 \\ 222 \\ 319\end{matrix} = \begin{matrix}15 \\ 14 \\ 7\end{matrix} \pmod{26},$$

{\displaystyle {\begin{pmatrix}6&24&1\\13&16&10\\20&17&15\end{pmatrix}}{\begin{pmatrix}0\\2\\19\end{pmatrix}}={\begin{pmatrix}67\\222\\319\end{pmatrix}}\equiv {\begin{pmatrix}15\\14\\7\end{pmatrix}}{\pmod {26}}}which corresponds to a cipher text of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{matrix}0 \\ 2 \\ 19\end{matrix}$$

{\displaystyle {\begin{pmatrix}6&24&1\\13&16&10\\20&17&15\end{pmatrix}}{\begin{pmatrix}2\\0\\19\end{pmatrix}}\equiv {\begin{pmatrix}31\\216\\325\end{pmatrix}}\equiv {\begin{pmatrix}5\\8\\13\end{pmatrix}}{\pmod {26}}}

This time, the enciphered vector is given by:

$$\begin{matrix}6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15\end{matrix} * \begin{matrix}2 \\ 0 \\ 19\end{matrix} = \begin{matrix}31 \\ 216 \\ 325\end{matrix} = \begin{matrix}5 \\ 8 \\ 13\end{matrix} \pmod{26}$$

which corresponds to a cipher text of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption

In order to decrypt, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). (There are standard methods to calculate the inverse matrix; see matrix inversion for details.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

$$\begin{matrix}6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15\end{matrix}^{-1} = \begin{matrix}8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8\end{matrix} \pmod{26}$$

{\displaystyle {\begin{pmatrix}6&24&1\\13&16&10\\20&17&15\end{pmatrix}}^{-1}\equiv {\begin{pmatrix}8&5&10\\21&8&21\\21&12&8\end{pmatrix}}{\pmod {26}}}

Taking the previous example cipher text of 'POH', we get:

$$\begin{matrix}8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8\end{matrix} * \begin{matrix}15 \\ 14 \\ 7\end{matrix} = \begin{matrix}260 \\ 574 \\ 539\end{matrix} = \begin{matrix}0 \\ 2 \\ 19\end{matrix} \pmod{26},$$

{\displaystyle {\begin{pmatrix}8&5&10\\21&8&21\\21&12&8\end{pmatrix}}{\begin{pmatrix}15\\14\\7\end{pmatrix}}\equiv {\begin{pmatrix}260\\574\\539\end{pmatrix}}\equiv {\begin{pmatrix}0\\2\\19\end{pmatrix}}{\pmod {26}}}which gets us back to 'ACT', just as we hoped.We have not yet discussed two complications that exist in picking the encrypting matrix. Not all matrices have an inverse (see invertible matrix). The matrix will have an inverse if and only if its determinant is not zero.

4. Observations and Results

We have tested our system on various images, encrypted them and again extracting them by decryption. Following are the 2 examples out of many.

Test 1

The **Figure 4** shows an original input image that is to be encrypted by Hill Cipher method

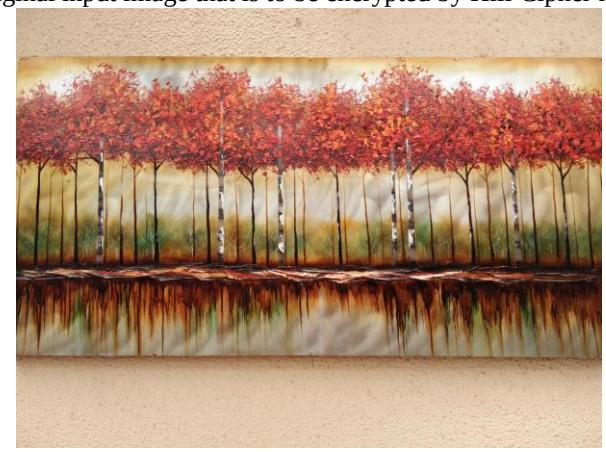


Figure 4; Original Image.

The **Figure 5** shows the encrypted image **Figure 6** shows the image after decryption.

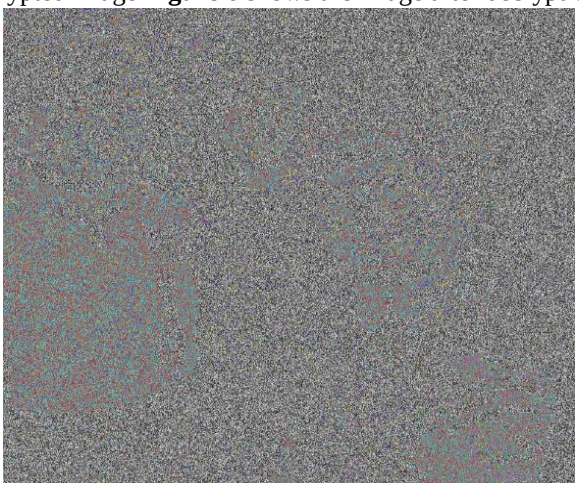


Figure 5; Encrypted image.

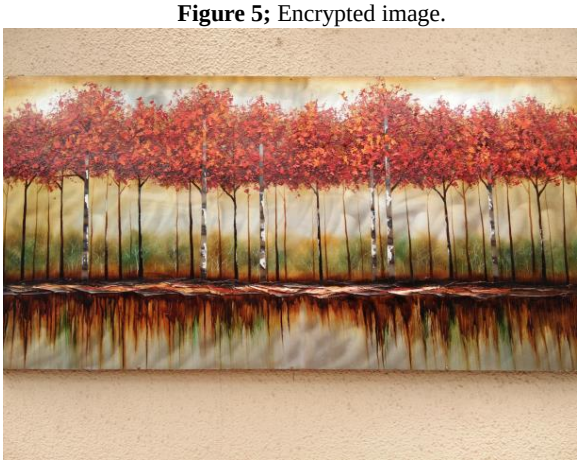


Figure 6; Decrypted Image.

4.2 Test 1

The **Figure 7** shows an original input image that is to be encrypted by Hill Cipher method

Figure 7; Original Image.

The **Figure 8** shows the encrypted image **Figure 9** shows the image after decryption.

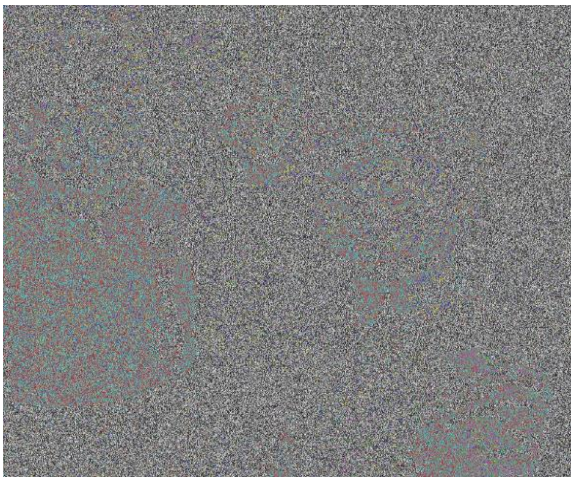


Figure 8; Encrypted image.

Figure 9; Decrypted Image.

Data Encryption and Decryption using Hill Cipher Method in MATLAB is shown in **Figure 10** and **Figure 11** respectively.

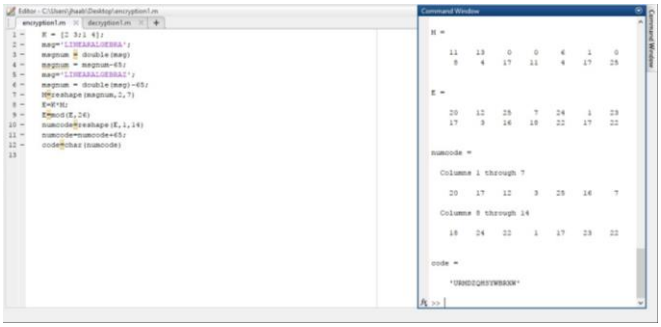


Figure 10; Data encryption using hill cipher method.

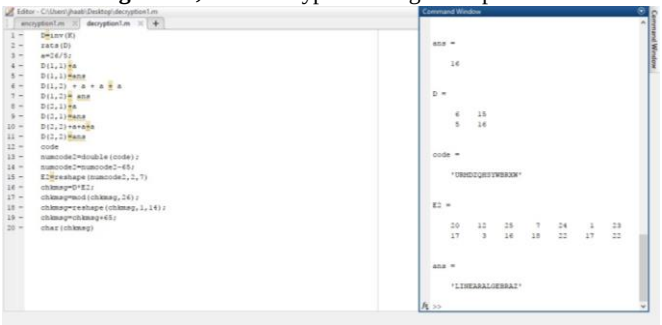


Figure 11; Data decryption using hill cipher method.

5. Conclusion and Future Scope

In this project separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases by using Hill-cipher method. Here we include another key act as password to decrypt the encrypted image. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image 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. In future, we implement this process of image encryption and data hiding in video sequence efficiently.

References

1. Zhang X. Revesible data hiding in an encrypted image. IEEE Signal Process 2011; 18(4): 255.
2. Johnson PE. IEEE Trans Signal Process 2010; 52.
3. Liu WZ. Efficient compression of encrypted image 2010; 19.
4. Tian J. Reversible data embedding using difference expansion. IEEE Trans Circuits System Video Technology 2003; 13(8): 890-896.
5. Shreya MS, Sandeep KS. Separable reversible data hiding in encrypted image using modified least significant bit and virtual embedding. International Journal of Science and Research (IJSR) 2013.
6. Rini J. Study on separable reversible data hiding in encrypted images. International Journal of Advancements in Research & Technology 2013; 2(12).
7. Qian Z, Han X, Zhang X. Separable reversible data hiding in encrypted images by n-nary histogram modification. 3rd International Conference on Multimedia Technology(ICMT 2013) 2013.
8. Jagadeesan J, Chelliah BJ, Nikhila N, et al. Reversible data hiding in encrypted images using AES data encryption technique. International Journal of Emerging Research in Management &Technology 2014; 3(4).