Secret Sharing using Image Hashing

Khaled Ahmed Nagaty
Faculty of Informatics and Computer Science Ain Shams University, Abbasia, Cairo, Egypt The British University in Egypt
El-Sherouk City, Cairo, Egypt

ABSTRACT
This paper presents a cryptographic technique that encrypts secret information using a coding image by transforming the pixels of this image from the intensity domain to the characters domain using a hash function. In the proposed technique, the coding image will be used to encrypt the secret information at the sender and decrypt it at the receiver using the pixels whose intensity values are transformed to characters. A matrix of characters corresponding to the coding image is generated where each character in this matrix corresponds to a pixel in the coding image and each character in the secret information is mapped to a character in the matrix of characters. The locations of characters in the matrix of characters that correspond to pixels in the coding image and correspond to characters in the secret information forms the pixels map. The pixels map is encrypted using a secret key before being sent to the receiver on a secure communication channel different from that used to send the coding image and at different times. Upon receiving the coding image and the encrypted pixels map the receiver uses the secret key to decrypt the pixels map and uses the coding image and the hash function to generate the matrix of characters. Each location in the pixels map is used to retrieve a character from the matrix of characters in order to decrypt the secret information. Experimental results showed the effectiveness and the efficiency of the proposed algorithm where a message was encrypted using a coding image without modifying its pixels and it was decrypted without errors.

General Terms
Security, Algorithms, Steganography, Cryptography.

Keywords
Secret sharing, Image pixels, Image transformation, Cryptography, Steganography, Information, Data hiding

1. INTRODUCTION
Cryptography is defined as the science of secret writing and it is used by Egyptians 4000 years ago to encipher hieroglyphics. Cryptography was very important to the military and diplomatic communications in the past, and recently it attracted much commercial attention due to the rapid growth of information age especially in storage, transmission, and spyware and that most systems are using the Internet. When sending a message over the Internet packet sniffers software can see any information that reaches their network card, as if you are sending a private message on a postcard through post mail where everyone in the post office can read it. Cryptography algorithms protect data of individuals from being disclosed or misused intentionally or unintentionally by encrypting so that an observer cannot understand what the data exactly mean. The aim is to modify the secret message to be imperceptible so that it does not leak any information about the embedded message itself. Traditionally there is one sender and one receiver and a passive eavesdropper who wants to disclose the secret message. A lot of messages that may contain vital information are sent between customers and organizations and between organizations themselves where many secure related actions are taken based on these messages. In this scenario cryptography techniques use secret keys to encrypt the data or the message before being sent to the receiver. An encryption algorithm is needed at the sender to encrypt a secret message using a secret key which when received the receiver decrypts the secret message using a decryption algorithm by using the same secret key used at the sender. Public keys allow a sender to send secret information to a receiver whose public key is authentic. A public key system can also be used to sign documents digitally. On the other hand, steganography is defined to be the hiding of writing, however in information hiding means that using another common medium such as an image or sound to hide the secret message into it [1,2]. Steganography embeds a secret message into another message which is more extensive and serves as a coding to the first message [17]. The goal is to modify the coding message to represent the secret message in an imperceptible way only, so that it does not leak any information about the embedding method nor about the embedded message itself. Image steganography techniques use images as a digital coding for hiding secret messages or data. Also, a secret key can be used to encrypt the data or the message before being embedded into the image. An embedding algorithm is needed to insert the secret message into the coding image at the sender which when received the receiver extracts the secret message using an extraction algorithm and by using the same secret key at the sender he/she decrypts the extracted message. The effectiveness of steganographic technique depends on how it is difficult to detect the existence of message in the image which can be noticed from changes of pixels intensities or colors due to the insertion of the message into these pixels. Another factor to measure effectiveness is the payload capacity by which maximum information can be embedded into an image without making any distortion that could be noticed. Also, the robustness of the steganographic algorithm measures the resistance of this algorithm against the extraction of embedded information [4]. The proposed algorithm satisfies all the three measures as the image is used as a digital coding but without embedding information into it which means that distortions cannot be made to the coding image. Also, by using the proposed algorithm large messages can be

encrypted without making distortions and without being noticed by a third party. Regarding robustness, the proposed algorithm is robust against any endeavors from a third party to decrypt the secret information because each time the algorithm is used to encrypt the same message or data using the same coding image another set of locations from the matrix of characters are chosen which makes it difficult for an observer to predict where the message or data can be. Moreover, separating the coding image from the file containing the locations of the pixels that are transformed to characters and sending each one on a separate communication channel increases this robustness, because an observer or a third party should acquire the image, the encrypted pixels map and the secret key used to decrypt the pixels map in order to fully recoding the secret information. This will be difficult if the coding image and the pixels map are sent separately using different communication channels in different times.

2. RELATED WORK

In cryptography there is no work that conceptually similar to the proposed algorithm. In stegnagoraphy which is the process of hiding data into images without any noticeable intensity degradation [3]. Steganographic techniques that change the coding images in order to embed secret information include the following:

• Spatial domain: These techniques hide the information in the least significant bits (LSB) of the image pixels because any change in these bits may be considered random noise and they cause the minimum distortion in the pixel [5].

• Transform domain: These techniques embed information in the frequency domain of an image. They are considered more powerful than the spatial domain methods because they embed information in the areas that are less exposed to image processing operations [6]. In [7], Jsteg employs the LSB setganographic technique to hide secret messages in a coding image by replacing the least significant bits of non-zero quantized DCT coefficients with secret message bits. However, JPHide, does not only modify the LSBs of a randomly selected quantized coefficients but also bits of the second least-significant bit-plane can also be changed [8]. In [9], Westfeld introduced the F5 steganographic algorithm where the quantized DCT coefficients are reduced by one rather than replacing their LSBs with the message bits. Also, the F5 algorithm uses a matrix embedding approach in order to reduce the number of modifications required for message hiding of a specific length. Wavelets are preferred for image steganography than DCT method because wavelets partition the high-frequency and low-frequency information on a pixel by pixel basis [10]. In [11,12], the authors presented a steganography technique which is based on wavelet compression. In [13], the authors used Linde-Buzo-Gray (LBG) vector quantization, associated with block codes, and one-stage discrete Haar wavelet transforms to produce good quality steganography images with little perceptual distortions. In [14], the authors used artificial neural networks technology for steganography. In [15], the authors used Discrete Wavelet Transform (DWT) to hide information.

• Spread spectrum: it deals with the coding image as noise or adds to the coding image pseudo-noise [4]. When dealing with the coding image as noise there are two techniques: the first one is the direct-sequence spread spectrum steganography where the coding image is divided into non-overlapped sub coding images. The second technique is the frequency-hopping spread-spectrum steganography where sub images consist of separate points are distributed over the coding image [16]. In pseudo-noise steganography the hidden information is distributed across the coding image which makes it difficult for an attacker to detect it [18]. In [19], Marvel et al., proposed a method to hide secret information into a coding image that combines spread spectrum communication, error control coding, and image processing techniques. In [20, 21], the authors used a technique to transmit hidden information by increasing the number of Fourier coefficients In [22], the authors described a blind image steganography, to retrieve the hidden information or message without using the coding image. The authors used a hybrid direct sequence/frequency hopping (DS/FH) technique.

• Statistical methods: They are known as model-based techniques because they modify the statistical characteristics of an image while keeping them in the embedding process. These modifications are small and cannot be noticed by human eyes that are weak in detecting luminance variation [23]. In [24], the authors use the least significant bit to embed a bit of data in the digital coding image. The statistical property of the coding image is changed if a "1" is transmitted and left unchanged otherwise. In [16], the authors divide the coding image into sub-images each corresponds to a single bit of the message. In [25], the authors proposed a data masking technique where the message signal is processed to view the properties of an arbitrary coding signal. In [26], the authors divided the coefficients of the transformed image into two parts where the coded message replaces the insignificant perceptually components. This leads to modify the statistics of the quantized non-zero AC DCT coefficients taking into consideration the parametric density function. A low precision histogram of each frequency channel is required in addition to matching each histogram with the model by deciding the corresponding model parameters.

• Distortion techniques: These techniques describe information by distorting the coding signal. So, knowledge of the coding coding image is important to these techniques where the encoder function adds sequence of changes to the coding coding image while the decoder function uses the differences between the coding coding image and the distorted coding image to restore the hidden information [4]. These techniques create stego-images by making a sequence of modifications to the coding image.

- File Embedding: These techniques hide secret information either in the header or at the end of the file [27].
- Palette Embedding: secret information can be hidden in the palette. Ordering of colors in the palette is used to hide information in the palette. The difference between two colors is used to embed a secret message in the palette, which means that one bit of the secret message for every two colors in the palette [4].

3. MOTIVATION

Cryptography techniques use only secret keys to encrypt secret messages and use the public key system for digital signatures. In the proposed cryptographic algorithm a secret key and coding image are used to encrypt secret messages which improve data security, integrity, confidentiality and privacy. Steganography techniques embed information in the coding image itself which may cause distortions to its pixels and a third party might be able to detect where the information is hidden. Modifications can be easily detected by the receiver if an attacker tampered with the stego-image either by cropping, rotating, or scaling. The coded secret message can be easily recodinged by simply reversing the

changes made by error correcting information used to encode the secret message [16]. In the proposed cryptographic technique, the coding image is used as a cover channel but without modifying its pixels. The intensities of the pixels in the coding image are transformed to characters and the locations of the pixels that correspond to characters in the secret message are determined and saved to a file called the pixels map. To increase security this pixels map is encrypted using a secret key. The encrypted pixels map and the coding image are sent to the receiver at different times using different secure communication channels which improves the safety and robustness of the proposed algorithm against steganographic and cryptographic attacks. By using the proposed algorithm the sender can use any type of image to send the secret information which is unlike steganographic techniques that prefer using the JPEG image type because it is commonly used on the Internet. Even if an attacker knows that the coding image being sent on a communication channel is used to encrypt secret information, the image itself will not reveal any information without acquiring the associated pixels map which is supposed to be sent on another secure communication channel and encrypted. Image steganography have a conflict between hiding information in high frequency areas to make it invisible to human eyes but in the same time it can be easily smoothed out using low pass image filters. Although hiding information in low frequency regions makes it more robust against low pass filters but they can be easily detected by human eyes. The proposed algorithm solved this conflict because the coding image is not used to hide the secret information but only to encrypt it. Moreover, the coding image in the proposed approach can be used more than once to encrypt many secret messages which is unlike conventional methods where an image is used only once due to the distortion of its pixels.

This paper is organized as follows: section 4 describes the proposed cryptographic algorithm, section 5 is dedicated to experimental results and section 6 is dedicated for conclusions.

4. PROPOSED CRYPTOGRAHIC ALGORITHM

The proposed algorithm is using two layers of security to keep data privacy, confidentiality, integrity and security. Fig.1 shows the framework of the overall cryptographic process using the proposed algorithm. The system encrypts the data using the coding image at the sender and decrypts it using the same image at the receiver. Firstly, the sender selects an image to be the coding image then by using the proposed cryptographic algorithm he/she encrypts the secret message using this image. The output of this process is the pixels map which contains the locations of the characters in the matrix of characters which correspond to the pixels in the coding image. For decrypting the secret data, the receiver uses the secret key to decrypt the pixels map and uses the received coding image to generate the matrix of characters. The characters in the matrix of characters can be accessed using the locations retrieved from the pixels map and consequently the secret message can be decrypted. Without the coding image, the secret key and the encrypted pixels map the secret information cannot be decrypted. This ensures the confidentiality, privacy and integrity of the data. In the following subsections the proposed cryptography algorithm is explained where in subsection 4.1 a pixel hashing function is described and in subsection 4.2 the generation of the matrix of characters is described and finally in subsection 4.3 the core algorithm is explained.

4.1 Pixel Transformation

The ASCII code for the characters "a-z" is [97-122], for "A-Z" is [65-90] and for a space ' ' is 32. The intensity of each pixel $I(x, y)$ is input to the hash function $h(I(x, y))$ then the following cases exist:

1. $v = I(x , y) \bmod 26$ ……(1)
2. If $I(x , y) \in [65\text{-}90] \parallel I(x, y) \in [97\text{-}122] \parallel I(x, y) = 32$
   return the character corresponds to $ASC(I(x, y))$
3. If $90 < I(x , y) < 97$
   return the character corresponds to $ASCII(v + 97)$
4. If $I(x , y) > 122$
   return the character corresponds to $ASCII(v + 97)$
5. If $I(x, y) < 65$
   return the character corresponds to $ASCII(v + 65)$

Where ASCII is a function that returns the character represented with the input decimal code and 26 is the number of English language characters. Numbers and special characters can be added to the matrix of characters by including their ASCII values in the hash function.

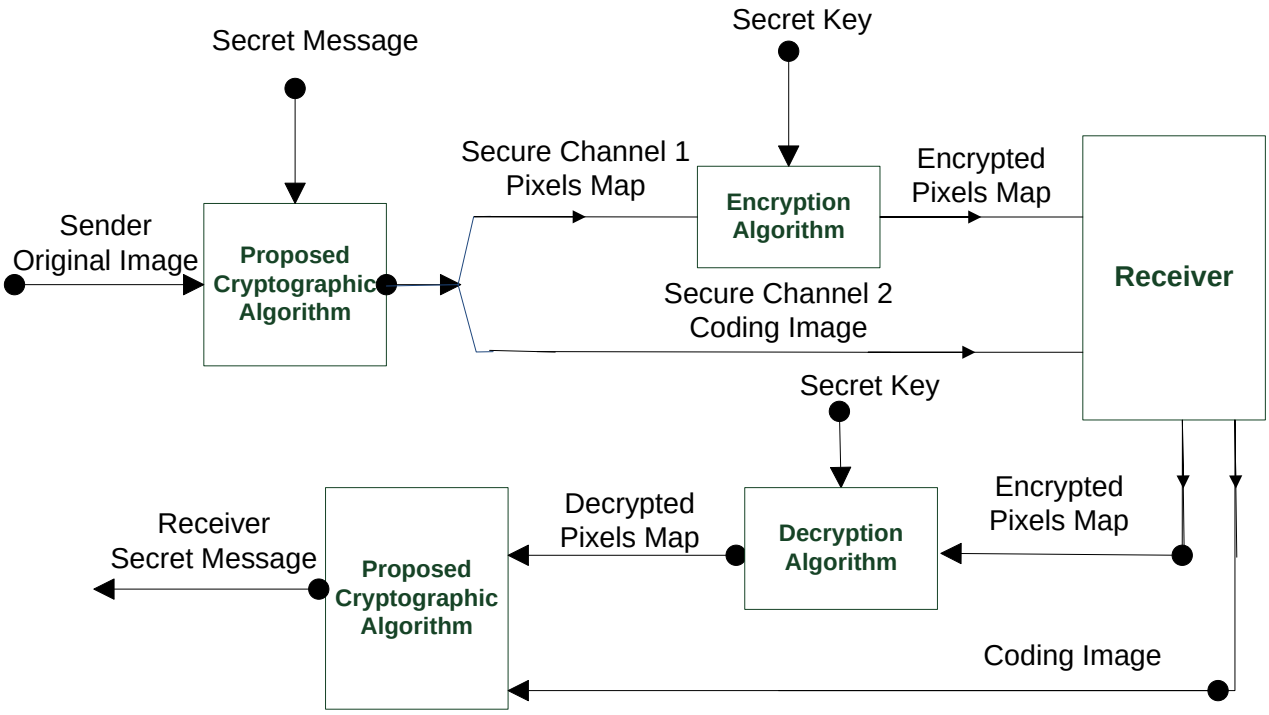

Fig 1: The framework for the proposed cryptographic algorithm

4.2 Matrix of characters

Input: A colored channel image.
Output: A matrix of characters.
Begin

1. Scan the image row by row.
2. Apply the pixel hash function in section 2 on each pixel of this image.
3. Return the character corresponds to the intensity of the pixel.

End

Fig 3 shows a part of the matrix of characters generated from the image of Fig. 2 [28] by using the algorithm in section 4.2. Notice that some pixels where transformed to small letters while others are transformed to capital letters. Empty entries in this matrix correspond to spaces. These are the spaces that will be mapped to spaces in the secret message.

Fig 2: Image of size 693 x 672 pixels

4.3 The core algorithm

Inputs: Coding image, Control random number generator, Secret message, Secret key.
Output: Pixels map.
Begin

1. Divide the RGB image into three channels (Red, Green and Blue).
2. Select an image with a specific colored channel image to be used as a coding image.
3. Generate the matrix of characters corresponding to the coding image.
4. Repeat
   4.1 Get a character from the secret message.
   4.2 Use the control random number generator to get a location in the matrix of characters. This generator is uniformly distributed to guarantee that the locations are spread uniformly across the matrix.
   4.3 Test if the generated location contains the required character and not used by another character from the message.
   4.4 If the test in step 4.3 is "TRUE" then save the coordinates of this location to the pixels map and set the flag "ON".
   4.5 If the test in step 4.3 is "FALSE" then the control random generator is called again to generate the coordinates of another location and go to step 4.3.
   Until end of input
5. Encrypt the output pixels map using the secret key.
6. Send the coding image using the secure communication channel 1 at time *k.*
7. Send the encrypted pixels map using the secure communication channel 2 at time *m*, such that $m \neq k$.

End

A flag is associated with each location in the matrix of characters to avoid collisions of the same characters using same locations in the matrix. If this flag is "ON", this means that this location is used by another character and the control random number generator is called to find another location in the matrix of characters.

4.4 Extracting secret information

Input: Colored channel image, Secret key, Encrypted pixels map;
Output: The secret message.

Begin
1. Decrypt the pixels map using the secret key.
2. Generate the matrix of characters for the input colored channel image.
3. Repeat
   3.1 Read a pair of coordinates from the pixels map.
   3.2 Read the pixel intensity from the channel image at the specified pair of coordinates.
   3.3 Transform the pixel intensity to a character using the hash function in section 4.1.
   3.4 Write the character to an output buffer.
   Until end of pixels map file
End

Fig 3: A part of the matrix of characters generated from the image of Fig 2.

5. EXPERIMENTAL RESULTS

To show the efficiency and effectiveness of the proposed algorithm the following colored image is used as a coding image to encrypt the following secret message: "***I want to meet you tomorrow***". The red colored channel image is used to encrypt that message although any colored channel image can be used to encrypt it. Several messages can be encrypted using the three colored channels at the same time, which means that a large amount of data can be encrypted and sent out without being noticed by a third party. Since the three colored channel images are independent of each other the algorithm can be easily parallelized. Fig. 4 shows the colored coding image of size 768x3072 pixels that was used for the message encryption.

Fig 4: Coding image

Fig. 5 shows the red, green and blue channel images for the image in Fig.4 each of size 768 x 1024 pixels.

Fig 5: Red, green and blue channel images for the image in Fig 4 each of size 768 x 1024 pixels

5.1 Simulation results

Tables 1 and 2 show the locations generated by the proposed algorithm which indicates where the characters of the secret message are located in the matrix of characters. Tables 3 and 4 show the pixels map to be encrypted and sent out to the receiver. Since the matrix of characters directly corresponds to the red channel of the coding image this means that the coordinates in the pixels map are the same coordinates of the pixels in the red channel image. Table 1 shows the locations of the characters after using the algorithm for the first time. Table 2 shows these locations after using the algorithm for the second time to encrypt the same message using the same red channel image. Notice that the locations are changed which means that whenever the algorithm is used new

locations for the characters of the message to be encrypted are generated. This means that the same coding image can be used many times and an attacker cannot predict from the image where the characters of the message are located.

Table 1. The coordinates of the characters in the red channel of the coding image First use of the proposed algorithm

Letter	**I**		**w**	**a**	**n**	**t**	
Row	138	717	392	274	427	460	715
Column	509	960	660	1015	969	734	999

Letter	**t**	**o**		**m**	**e**	**e**	**t**
Row	549	707	716	426	177	107	653
Column	364	276	996	809	956	463	766

Letter		**y**	**o**	**u**		**t**	**o**
Row	715	215	181	169	713	357	447
Column	967	357	356	804	959	106	455

Letter	**m**	**o**	**r**	**r**	**o**	**w**
Row	314	349	675	125	80	60
Column	25	426	411	736	793	838

Table 2. The coordinates of the characters in the red channel of the coding image Second use of the proposed algorithm

Letter	**I**		**w**	**a**	**n**	**t**	
Row	667	764	406	107	50	110	719
Column	961	925	811	212	680	113	980

Letter	**t**	**o**		**m**	**e**	**e**	**t**
Row	54	525	713	86	111	604	498
Column	613	1012	1001	567	77	825	69

Letter		**y**	**o**	**u**		**t**	**o**
Row	724	440	285	605	723	455	82
Column	953	529	208	736	952	363	730

Letter	**m**	**o**	**r**	**r**	**o**	**w**
Row	478	379	695	410	193	698
Column	934	276	797	461	324	720

Table 3. Pixels map for the coordinates of table 1 before encryption

138	717	392	274	427	460	715
509	960	660	1015	969	734	999
549	707	716	426	177	107	653
364	276	996	809	956	463	766
715	215	181	169	713	357	447
967	357	356	804	959	106	455
314	349	675	125	80	60	
25	426	411	736	793	838	

Table 4. Pixels map for the coordinates of table 2 before encryption

667	764	406	107	50	110	719
961	925	811	212	680	113	980
54	525	713	86	111	604	498
613	1012	1001	567	77	825	69
724	440	285	605	723	455	82
953	529	208	736	952	363	730
478	379	695	410	193	698	
934	276	797	461	324	720	

5.2 Discussion

In comparison with conventional techniques which use images as coding channels to send secret messages, the proposed technique does not hide the secret message directly into the coding image as conventional techniques do. Instead, pixels of the coding image are transformed from the intensity domain to a characters domain and a matrix of characters corresponding to those pixels is generated. Each character in this matrix corresponds to a pixel in the coding image with the same coordinates. This means that pixels of the coding image will not be changed or distorted as conventional techniques do. The proposed technique is believed to be more efficient than other techniques because the coding image I which is the input to the proposed technique will be the same as the output coding image I' which means that $I = I'$ this is because the coding image does not contain the secret information and accordingly its pixels are not changed. This means that the mean squared error is:

$$MSE(I,I') = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - I'(i,j))^2 = 0 \quad \text{.....(2)}$$

The peak signal to noise ratio is:

$$PSNR(I,I') = 10 \log_{10}(\frac{255^2}{MSE}) \text{dB} = \text{INF} \text{.....(3)}$$

On the other hand, the PSNR for coding images used by the technique presented in [29] has an average PSNR of 40.3 dB this is because the pixels of the image are modified to hide the secret information. The fidelity of the proposed technique is higher than other conventional techniques because $MSE(I,I') = 0$ and hence the secret information cannot be detected by the human visual system or statistical analysis. The output coding image I' contains only the original pixels of the coding image I which correspond to the characters in the matrix of characters and to the characters of the secret information. The pixels map which contains the coordinates of the pixels used in the encryption of the secret information is sent to the receiver after being encrypted with a secret key. The pixels map and the coding image are sent separated from each other using two different secure communication channels and in two different time slots. The encrypted pixels map, the coding image and the secret key required for the decryption of the pixels map are all required to decrypt the secret information. This makes the proposed technique more secure than other techniques. The payload of the proposed technique is considered very large because the three colored channels of the coding image can be used to encrypt information and each channel image contains a large number of characters which correspond to a large number of pixels in the channel image. The imperceptibility using the proposed technique is very large compared with the techniques in [29, 30]. In the proposed technique, there is no visual difference between the input coding image I and the output coding image I' because $MSE(I,I') = 0$ and $PSNR(I,I')$ = INF while in [29, 30] there is a visual difference between the cover image and the stego-image because the average PSNR = 40.3 dB and 39.18 dB respectively. An attacker will not benefit from the encrypted pixels map without the secret key required for the decryption of this map and the coding image. The proposed technique has very large payload compared to other conventional techniques because large messages can be encrypted using the input coding image I while still preserving very large imperceptibility because always $I = I'$ and $MSE(I,I') = 0$. In addition to a three colored channel images that can be used to encrypt secret information using the proposed technique. In conventional techniques, where the pixels of the input coding image are modified to embed information there is a limit on how many bits can be changed without reducing the imperceptibility of the output image which limits the payload of these techniques.

6. CONCLUSIONS

This paper proposed a cryptographic technique which uses a coding image to encrypt secret information by transforming the pixels of the coding image from the intensity domain to characters domain using a hash function. The output of this transformation is a matrix of characters where each character in this matrix corresponds to a pixel in the coding image. Each time a character is read from the secret information the matrix of characters is accessed to find a corresponding character. The location of this character in the matrix is stored in the file of pixels map. A secret key is used to encrypt the pixels map before sending it to the receiver. Both the coding image and the encrypted pixels map are sent separated from each other using different secure communication channels at two different times. The main advantage of this approach is that the coding image can be used many times unlike the coding images used by steganographic techniques which are used only once because of the distortions made to their pixels. Secret information is not hidden into the coding image and hence the proposed algorithm has high fidelity and imperceptibility which make it robust against visual attacks and computer analysis attacks. Security and privacy of data are improved as many security measures are taken, the receiver should obtain the coding image, the encrypted pixels map and the secret key required to decrypt this map. Using two different secure communication channels to send the coding image and the encrypted pixels map at different times reduce the possibility for an attacker to acquire both the coding image and the encrypted pixels map. Even if the attacker was able to obtain the coding image and the encrypted pixels map, he/she still needs the secret key to decrypt this pixels map which makes it harder for the attacker to break the proposed technique. Finally, the proposed technique has very high fidelity, very large imperceptibility and very large payload as each of the three colored channel images can be used to encrypt secret information. The pixels of each channel coding image are not modified and accordingly imperceptibility is not reduced by encrypting large size information.

7. REFERENCES

[1] B. Dunbar. 2002. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1.

[2] C. Christian. 1998. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science.

[3] M. Chen, N. Memon, E.K. Wong. 2008. Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts Methodologies, Tools and Applications, New York: Information Science Reference, 2008, 438-450.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi. 2012. "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2012, 168-187.

[5] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr). Image steganography: Concepts and practice. WSPC/Lecture Notes Series: 9in x 6in, [On line], pp. 1-49.Available on: http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf [Aug. 2011].

[6] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003). A survey of steganography techniques for image files. Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available on: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

[7] N.F. Johnson and S. Jajodia. (1998, Feb.). Exploring steganography: seeing the unseen. IEEE Computer Journal. [On line]. 31(2), 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[8] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. 2010. Digital image steganography: survey and analysis of current methods. Signal Processing Journal. [On line]. 90(3),727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[9] A. Westfeld. 2001. F5-A steganographic algorithm: high capacity despite better steganalysis. In Proc. of the 4th Information Hiding Workshop, LNCS, 2001, 289-302.

[10] H.S. Majunatha Reddy and K.B. Raja. (2009). "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security.[On line]. 3(6), 462-472.

Available:http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue6/IJCSS-163.pdf [Jun., 2011].

[11] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. 2000. Exploring on steganography for low bit rate Wavelet based coder in image retrieval system. In Proc. of IEEE TENCON, 2000, pp. 250-255.

[12] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao.2000. Steganography for low bitrate Wavelet based image coder. In Proc. of IEEE ICIP, 2000, pp. 597-600.

[13] N.K. Abdulaziz and K.K. Pang. 2000. Robust data hiding for images. In Proc. of IEEE International Conference on Communication Technology, 2000, 380-383.

[14] L.D. Paulson. (2006, Aug.). New system fights steganography. News briefs. IEEE Computer Society. [On line]. 39(8), 25-27. Available:http://journals2.scholarsportal.info/details.xqy?uri=/00189162/v39i0008/25_nsfs.xml [Jul.,2011].

[15] A.A. Abdelwahab and L.A. Hasan. 2008. A discrete Wavelet Transform based technique for image data hiding. In Proc. of 25th National Radio Science Conference, 2008, 1-9.

[16] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), A survey of steganography techniques for image files. Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

[17] A. Westfeld and A. Pfittzmann.1999. Attacks on steganographic systems- breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned. In Proc. of the 3rd Internet Workshop on Information Hiding, 1999, 61-76.

[18] H. Wang and S. Wang. (2004, Oct.). "Cyber Warfare: steganography vs. steganalysis."Communications of the ACM. [On line]. 47(10), 76-82. Available: www.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf [Mar., 2011].

[19] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. 1999. Spread spectrum image steganography. IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083. Available:http://www.mendeley.com/research/spread-spectrum-image-steganography-1/[Apr., 2011].

[20] F. Alturki and R. Merserau. 2001. Secure blind image steganographic technique using Discrete Fourier Transform. In Proc. IEEE International Conference on Image Processing, 2001 ,16-162.

[21] R.J. Anderson and F.A.P. Petitcolas. (1998, May). On the limits of steganography. IEEE Journal of Selected Area in Communications. [On line]. 16(4), 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[22] K.C. Widadi, P.H. C.C. Wah. Blind steganography using direct sequence/frequency hopping spread spectrum technique. Information, Communications and Signal Processing, 5th International Conference, 2006. pp. 1125-1129.

[23] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). "Image steganography: Concepts and practice." WSPC/Lecture Notes Series: 9in x 6in, [On line], pp. 1-49. Available: http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf. [Aug. 2011].

[24] S.C. Katzenbeisser. 2000. Principles of Steganography. In Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, 43-78.

[25] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. 2002. Data masking: a secure-coding channel paradigm. In IEEE Workshop on Multimedia Signal Processing, 2002, 339- 342.

[26] P. Sallee. 2004. Model-based steganography. In Proc. the 2nd International Workshop on Digital Watermarking, LNCS, 2004. , 254-260.

[27] Y.O. Yildiz, K. Panetta, and S. Agaian. (2007, Apr.). New quantization matrices for jpeg steganography." International Society for Optical Engineering. [On line]. 6579(1), pp. 6579OD. Available: link.aip.org/link/?PSISDG/6579/65790D/1. [Nov., 2011].

[28] IconArchive, 2013. Available: http://www.iconarchive.com/tag/file. Visited 18/07/2013.

[29] Pei-Yu Lin, Chi-Shiang Chan. 2010. Invertible secret image sharing with steganography, Pattern Recognition Characters 31, 1887–1893.

[30] Chang-Chou Lin, Wen-Hsiang Tsai. 2004 Secret image sharing with steganography and authentication, Journal of Systems and Software, Volume 73, Issue 3, November–December 2004, Pages 405-414