International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Energy Efficient and Secure Image Communication over Wireless Network

Amandeep Sharma[1], **Dr. Parvinder Kaur**[2]

[1, 2] MMEC MM University Mullana, Ambala, Haryana, India

Abstract: ***In this paper Wireless Sensor Networks (WSNs) are a collection of tiny nodes,. These nodes are typically battery-operated and their recharge or replacement may be undesirable or not possible. Thus, energy consumption is a key issue in the design of WSNs. The large amount of data traffic for image transmissions over a WSN can rapidly shorten the lifetime of the network, So a strategy to mitigate this problem is to promote some sort of image data compression. Recent works have investigated image transmission in WSNs, and many of them employ wavelet-based image compression. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Steganography method used in this paper is based on biometrics in skin tone region of images. Here secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. This study shows that by adopting collaborative method of compressed image communication we get energy efficient network.***

Keywords: Energy conservation, Image Communication, Steganography method and Wireless sensor network

1. Introduction

Maintaining the secrecy of digital information when being communicated over the internet is presently a challenge. Given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on cipher text. An ideal steganography technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of steganography is a method of embedding additional information into the digital contents that is undetectable to listeners.

We are investigating its embedding, detecting, and coding techniques. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision.

The new steganalytic approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed steganalytic approach, using a frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results in an enhanced security than hiding data without cropping i.e. in the whole image, so cropped region works as a key at decoding side. The study shows that by adopting an object oriented steganography mechanism, in the sense that, we track skin tone objects in an image, we get a higher security and energy efficient network. And also satisfactory PSNR (Peak- Signal-to-Noise Ratio) is obtained. This securely and efficiently compressed image can be transmitted using collaborative communication over wireless sensor network.

2. Discrete Wavelets Transform

The DWT is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale. DWT is computed with a cascade of filtering followed by a factor 2 sub sampling (Figure 1.)

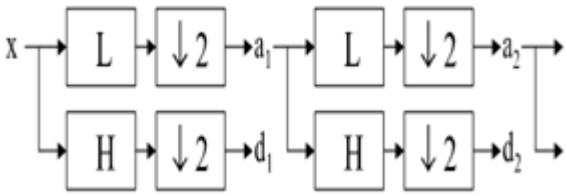

Figure 1: DWT tree

H and L denotes high and low-pass filters respectively, ↓ 2 denotes sub sampling.

Elements a1 are used for next step (scale) of the transform and elements d1, called wavelet coefficients, determine output of the transform. l[n] and h[n] are coefficients of low and high-pas filters respectively One can assume that on scale j+1 there is only half from number of a and d elements on scale j. This causes that DWT can be done until only two aj elements remain in the analyzed signal These elements are called scaling function coefficients . DWT algorithm for two-dimensional pictures is similar. The DWT is performed

firstly for all image rows and then for all columns (Figure 2.)

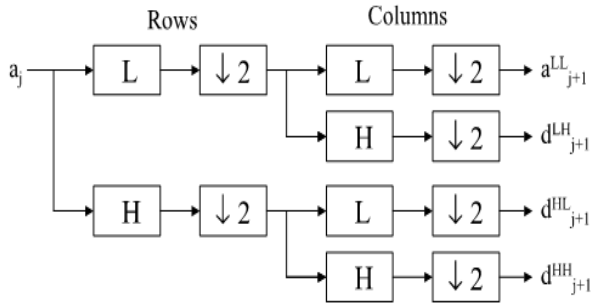

Figure 2: Wavelet decomposition for two-dimensional pictures

By using the wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal. Wavelets seem to be effective for analysis of textures recorded with different resolution [3].

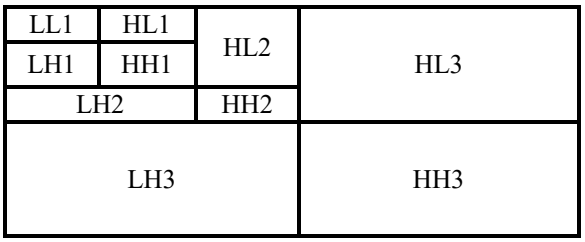

Figure 3: Sub band labeling Scheme for a Three Level, 2-D Wavelet

2.1 Wavelet Computation

In order to obtain an efficient wavelet computation, it is important to eliminate as many unnecessary computations as possible. A careful examination of the forward and reverse transforms shows that about half the operations either lead to data which are destroyed or are null operations (as in multiplication by 0).

The one-dimensional wavelet transform is computed by separately applying two analysis filters at alternating even and odd locations. The inverse process first doubles the length of each signal by inserting zeros in every other position, then applies the appropriate synthesis filter to each signal and adds the filtered signals to get the final reverse transform.

2.2 Algorithms and Transformations

Another steganography method is to hide data in mathematical functions that are in compression algorithms. Two functions are Discrete Cosine Transformation (DCT) and Wavelet Transformation. The DCT and wavelet functions transform data from one domain into another. The DCT function transforms that data from a spatial domain to a frequency domain.

3. Steganography

Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting [2] method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.

4. Proposed Methodology

Transmitter: The function of the transmitter is to transmit the secure image embedded with data to the receiver.

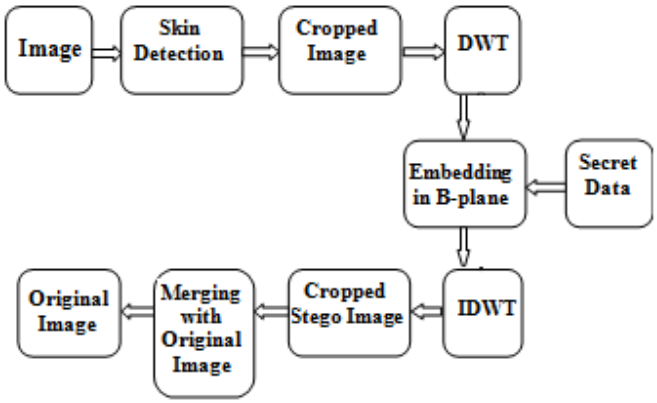

Figure 4: Secure and energy efficient image Transmitter

Receiver: Receiver receives the data by using cropped image as key for extraction of the image and secure data.

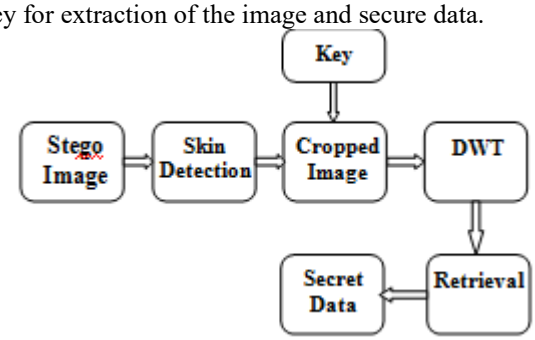

Figure 5 Secure and energy efficient image Receiver

5. Algorithm

Step 1:
Let the cover image is represented by c(x,y). It is then passed through a filter with transfer function H(X,Y) to separate high and low frequency components.

$$F[c(x, y)] = C(X, Y)$$

where C(X,Y) represents Fourier Transform of the cover image. In this paper capital letters representation for pixel is used for frequency domain and small letters for spatial representation.

$$C(X, Y)H(X, Y) = LO(X, Y) + HI(X, Y)$$

where LO(X, Y), HI(X, Y) represent low frequency and high frequency components of cover image respectively, obtained after passing through the filter with cut off as stated above.

Step 2:
Inverse transform of both the frequency components is found out, known as HFSI (High Frequency components Spatial Image) and LFSI (Low Frequency components Spatial Image) separately.

F1[LO(X, Y)]= lo(x, y) and
F1 [HI(X, Y)] = hi(x, y)

where lo(xy) and hi(x,y) are the spatial components of low and high frequencies in the cover image respectively.

Step 3:
Now message is embedded into HFSI image. The number of bits modified in a pixel is made to depend up on its magnitude and also on the local features of the cover Image. Let the message is represented as m(x,y) and the embedding function as M[]

mlo(x, y) = M[lo(x, y) + m(x, y)]

Step 4:
Both the modified HFSI and unmodified LFSI are added to form stego - image.
Steg(x, y) = mlo(x, y) + lo(x, y)

Step 5:
At the receiver LFSI is subtracted from stego - image leaving modified HFSI image. mhi(x, y) = steg(x, y) - hi(x, y)

Step 6:
Now the message is decoded from the Modified HTSI image using the stego – key

m(x, y) + lo(x, y) = M '[mhi(x, y)]

Simulation Results: These figures shows the simulation results of secure and energy efficient image transmission in different stages of simulation process.

6. Energy Consumption Conventioal Image

6.1 Least Significant Bit Insertion (LSB)

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

Simplified Example with a 24 bit pixel:

1 pixel:
(00100111 11101001 11001000)

Insert 101:
(00100111 11101000 11001001)
red green blue

Simplified Example with an 8 bit pixel:

1 pixel:
(00 01 10 11)
white red green blue

Insert 0011:
(00 00 11 11)
white white blue blue

Advantages of LSB Insertion: A major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software developed which work around LSB color alterations via palette manipulation. LSB insertion also works well with gray-scale images.

6.2 Adaptive Steganography Using Filtering:

Adaptive Steganography reduces modifications to the image and adapts the message embedding technique to the actual content and features of the image. In general, to keep a good degree of stealth ness, Adaptive methods embed message bits into certain random clusters of pixels (avoiding areas of uniform color) selecting pixels with large local standard deviation or image blocks containing a number of different colors. The main advantage of adaptive steganography is that the changes made to the cover image take into account the sensitivity of the human visual system and also various statistical parameters generally being used by steg-analysis algorithms. The main challenge posed to existing adaptive steganography techniques [3,4,5,6] is that the methods so far developed doesn't seem to have a way to control the amount of information that is to be hidden, for a given cover image. This problem is overcome in the method presented in this paper.

The proposed approach utilizes the sensitivity of the human visual system to adaptively modify the intensities of some pixels in a high frequency components spatial image (HFSI) of the cover image. The modification of pixel intensities depends on the magnitude of the pixels in HFSI and also on the local features of the cover image. If the contrast of the image is large (e.g., an edge), the intensities can be changed greatly without introducing any distortion to human eyes. On the other hand, if the contrast is small (e.g. smooth), the intensities can only be tuned slightly. In this method, first the cover image is passed through a filter to separate the high and low frequency components of the image. The inverse transform of both the images is computed. Now the pixels values of HFSI are modified depending on the magnitude of the pixel i.e. more the magnitude more the Least Significant Bits (LSB's) of that pixel are changed and also the local features of cover image are considered. Now both the LFSI (Low Frequency components spatial image of cover image) and HFSI are added to form the stego - image. At the receiver the reverse process is to be done to recover the message.

6.2 Least Significant Bit Insertion

Usually 24-bit or 8-bit files are used to store digital images. The former one provides more space for information hiding. however, it can be quite large. The colored representations of the pixels are derived from three primary colors: red, green and blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data, then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system. This simple method is known as Least Significant Bit insertion. Using this method it is possible to embed a significant amount of information with no visible degradation of the cover image.

6.3 Proposed Scheme

Collaborative-DWT

We consider applications where, although high quality images are preferred, images with lower quality are tolerable. This way, we proposed an collaborative-DWT scheme, based on the classical collaborative protocol, however, instead of retransmitting the entire image, in the collaborative transmission only a lower-resolution version of it. As mentioned in Section II, when the 2D-DWT is applied to an image, four sub-bands are produced, with sub-band corresponding to a quarter-size version of the original image. Applying the 2D-DWT again over sub band produces the sub-band which is, by its turn, a quarter-size version of the sub-band image, corresponding to an image which is 1/16 times smaller than the original one. This decomposition procedure could be done many times as desired, but at the expense of a lower image quality. The resulting total consumed energy per bit in the proposed Collaborative image transmission.

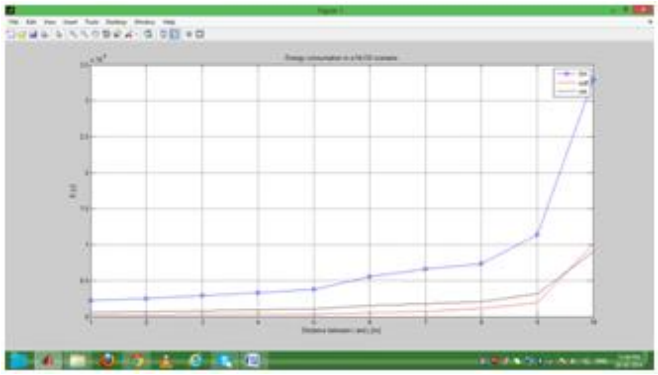

Figure: 6 Comparison between Single hop, Multihop and Collaborative Technique

7. Conclusion

In this paper we have presented a new method of steganography with higher embedding capacity. The embedding capacity of the approach is controlled through the filter cut-off frequency. The approach was analyzed and shown to have a very high confidentiality due to the sharpness of information recovery with the cut-off frequency.

In this paper, we have proposed a new steganographic scheme to hide secret message in digital images. The proposed scheme embeds the secret message by modifying the wavelet coefficients of the original cover image. Moreover, the modification is based on the patterns of the wavelet coefficients. The experimental results show that the difference between the original image and the embedded image is visually unnoticeable and the embedded message could be extracted properly following the proposed extracting procedure. And In this thesis we also investigated the energy efficiency of an image transmission in a simple WSN scenario combining wavelet multilevel decomposition with an ISDF Collaborative scheme. We show that the proposed scheme is more energy efficient than single-hop and multi-hop cooperative schemes, with a negligible decrease of overall image quality.

References

[1] H. Ochiai , P. Mitran , H. V. Poor and V. Tarokh "Collaborative beam forming for distributed wireless ad hoc sensor networks", IEEE Trans. Signal Processing, vol. 53, no. 11, pp.4110 -4124 2005

[2] E. B. Manhas , G. Brante, R. D. Souza and M. E. Pellenz, "Energy-Efficient Cooperative Image Transmission over Wireless Sensor Networks" 2012 IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks. pp. 2014-2019.

[3] J. L. Jun Cheng, Alex C. Kot and H. Cao, "Steganalysis of Data Hiding in binary Text Messages," in ISCAS, May 2005, pp. 4405-4408.

[4] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image Steganography", in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg. of Computer Based Systems (ECBS'08), Belfast, 2008, pp. 159-168.

[5] Q. Zhengding and F. Dervai, "A new wavelet feature for wavelet basis selection in wavelet-fractal hybrid image coding," in Signal Processing Proceedings, 2000. WCCC-ICSP 2000. 5th International Conference on, 2000, pp. 1054-1057 vol.2.

[6] Chaabouni I., Image compression with Self Organizing Maps, IJCIIS, January 2010 Issue, pp64-71.

[7] Mauro Barni, Franco Bartolini, Enrico Magli and Gabriella Olmo, "Watermarking techniques for electronic delivery of remote sensing images", Optical Engineering, 41, No. 9, pp. 2111-2119, September 2002.

[8] Jar no Mielikainen, "LSB Matching Revisited", Signal Processing letters, IEEE, vol. 13, issue 5, pp. 285-287, May 2006.

[9] M. Kociołek, A. Materka, M. Strzelecki P. Szczypiński Discrete wavelet transform –derived features for digital image texture analysis, Proc. of Interational Conference on Signals and Electronic Systems, 18-21 September 2001, Lodz, Poland, pp. 163-168.

[10] Artz D., "Digital Steganography: Hiding Data within Data", Internet Computing IEEE, vol. 5, issue 3, pp. 75-80, 2001.

Author Profile

Amandeep Sharma received the B-tech. degrees in Electronics and Communication Engineering from SKIET(KURUKSHETRA) in 2009 and pursuing his M.Tech in ECE from MMU, Mullana, Ambala, Haryana. His field of interest is in MATLAB secure and energy efficient image Transmission. Presently the author 1 working as Project Engineer In L&T EBG in Chandigarh.