ISSN: 0974-6471, Vol. 10, No. (4) 2017, Pg. 817-823

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Steganography Based on Human Perception

SUMAN CHAKRABORTY[1]* and ANIL BIKASH CHOWDHURY[2]

[1]Research Scholar of Techno India University, India.
[2]Head of the Department of Computer Application, Techno India University, India.

Abstract

Today internet has become a trusted factotum of everyone. Almost all payments like tax, insurance, bank transaction, healthcare payment, payment in e-commerce are done digitally through debit or credit card or through e-wallet. People share their personal information through social media like Facebook. Twitter, WhatsApp etc. The government of every developing country is going to embrace e-Governance system to interact with people more promptly. The information shares through these applications are the burning target to intruders. This paper utilized the imperceptibility as well as the robustness of steganography techniques which are increased by embedding multiple bits in a particular region selected either based on some image attributes or by Human Visual Perception.

Article History

Received: 14 December 2017
Accepted:21 December 2017

Keywords

Security,
Hiding Data,
Steganography and
Human Perception.

Introduction

In the field of Data Communication, security-issues have got the top priority. So, of late the degree of security provided by a security tool has become the main evolutionary criteria of it. Classical cryptography is one of the ways to secure plain text messages. Along with that at the time of data transmission, security is also implemented by introducing the concept of steganography, watermarking, etc. In this types of combined approach, there exits some drawbacks. In remote networking, at the time of transmission of hidden encrypted text message, if the eavesdroppers get the track of the hidden text, then they could easily get the encrypted text. Now breaking of encrypted text message can be achieved by applying some brute force technique. So, there remains some probability of snooping of information. So, this type of techniques incurs another level of security which can route the Crypto-analyzer or Stegoanalyzer in a different direction.

Different techniques are already plays an important role in the field to information security for a long decade. The famous one is cryptography that keeps the content of the message secret, but it is not sufficient at all. On the other hand the watermarking hides data to keep copyright related information[1-2]. It is also not secure at all because many techniques are available to remove watermark easily. Now-a-days people prefer a system that hides

CONTACT Suman Chakraborty ✉ 1954samir@gmail.com Research Scholar of Techno India University, India.

To link to this article: http://dx.doi.org/10.13005/ojcst/10.04.17

the existence of message secret. The technique, Steganography highlights the concept of security through obscurity.

The word “Steganography” is the combination of two Greek words Stegano(Cover) and Grafia(Writing) and its aim is “to hide in plain sight”[3]. It has been used throughout 2500 years and was coined at the end of the 15th Century after the appearance of Trithemius book on the subject “Steganographia”. Modern steganography is generally understood to deal with electronic media rather than physical objects. The synopsis introduces noble methods of steganography by considering Image and Audio as cover media.

The rapid use of digital images for communication through internet makes image a popular cover media in steganography. Not only this reason, there are some other factors like content adaptability, redundancy, limited power of HVS, continuous growth of strong graphics power in computer, and the fruitful contribution of the researcher in the field of digital image processing also stand behind this popularity[4]. The reason for considering audio as cover media is the representation of amplitudes in real number format causes very small distortions after embedding the bits of target data. Instead of that the audio also has some unique characteristics like gradual change in amplitudes rather than sudden change, high frequency suppress lower frequency components etc., whereas the strong sensitivity of Human Auditory System (HAS) makes audio steganography a more challenging security technique[5].The proposed work designs some new approaches which are efficient and gives researchers an opportunity to come up with new ideas in information security.

Literature Survey

The better understanding on different state-of-the-art works is very helpful for the validation of new implementation and also analyzing its performance accuracy in terms of security. The synopsis starts with the solution of the loopholes of standard LSB technique and then tries to enrich the thoughts. The standard LSB technique is very easy to implement where the Least Significant bit of a pixel/samples of cover media is replaced with target bit[6]. The method can preserve imperceptibility but suffers from low robustness and capacity. T. Penvy et al. introduce a secure steganography algorithm HUGO which can able to defeat almost all steganalysis attacks by defining distortion based on feature vector already used in steganalysis. It supports capacity of stego media seven times more than standard LSB technique. However, the results were not satisfying at all in the case of multi-bit approach[7].

B. C. Nguyen *et al.,* improves the capacity of LSB substitution techniques by introducing popular multi bit-plane image steganography technique. The increase in capacity again reduces imperceptibility[8]. W. C. Kuo *et al.,* increases capacity by embedding multiple bits of target data encoded through run-length encoding (RLE), but maintain imperceptibility by considering Multi-bit Generalized Exploiting Modification Direction (MGEMD) characteristics. MGEMD features not only reduce distortion but help to resist modern steganalysis attacks[9]. The all above discussion does not meet robustness up to the level. The robustness of the LSB Substitution technique may increase by embedding data at higher LSB layer or through embedding at random positions of the cover and also introducing double layer security. N. Cvejic *et al.,* in their work embeds target data at the higher bit-plane then preserves quality through bit adjustment.

Proposed Method

Human visual perception is the ability to interpret the surrounding environment using light in the visible spectrum reflected by the objects in the environment. Color creates a clear sensation about an object to human eye. The color perception is a subjective process is controlled by three cone cells – "red" (64 %), "green" (32 %), and "blue" (2 %). The green and red cones are concentrated in the fovea centralis whereas the "blue" cones are mostly found outside the fovea but have highest sensitivity and leading to some distinctions in the eye's blue perception. The absorption and sensitivity curve in Figure 1 support this thought and it is suggested that some selective "blue amplifier" somewhere in the brain makes some boosting mechanism to blue light.

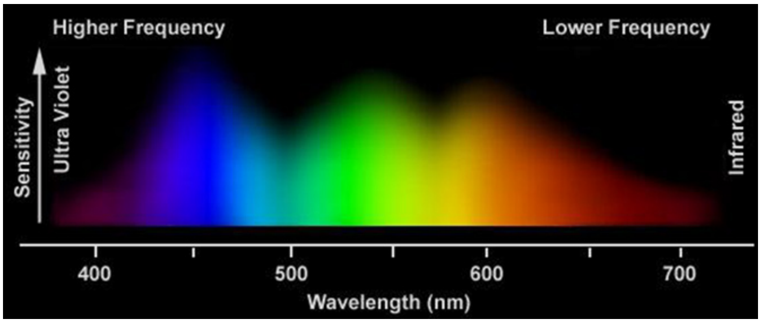


Fig. 1: Absorption and Sensitivity curve

The embedding is done on Red and Green Channel whereas the Blue channel keeps unchanged for region selection and channel selection during embedding at blue region. Human visual perception is more sensitive to blue color which claims more careful embedding at blue region than the embedding at non-blue region. In blue region the three target bits are embedded in each of the selected channel. In non-blue region three bits of target data are embedded in each color channel helps in the increase of capacity. The result and analysis shows that the method successfully meets three challenges of steganography. The results and analysis are shown in Figure 2 and Table 1.

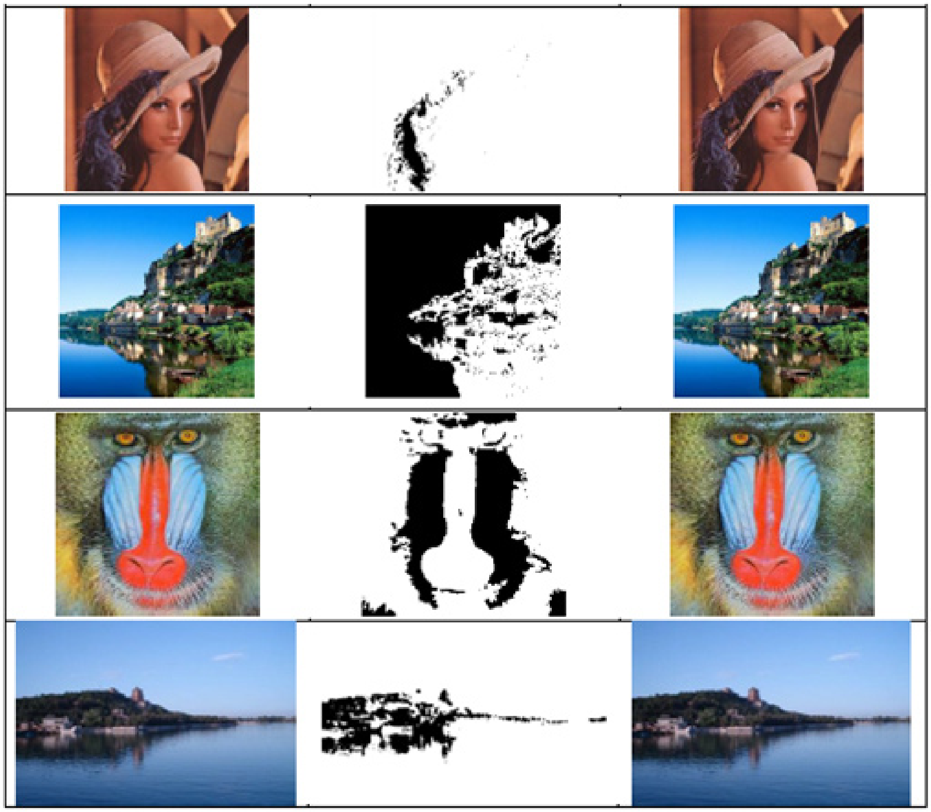


Fig. 2: Sample Results. Cover Images, Image with segmented Blue & Non-Blue Region and Stego Images

Table 1: Result Analysis based on PSNR, LMSE and SSIM

Image	Perc. of blue reg.	Perc. of non-blue reg.	Capacity (bpp)	Embadding in blue reg	Embadding in non-blue reg	PSNR R	PSNR G	LMSE	SSIM
Lena	15	63	4.23	40%	40%	42.95	42.94	0.0089	0.9984
				100%	100%	39.77	39.16	0.0223	0.9964
Baboon	59	39	4.11	40%	40%	44.09	43.42	0.0103	0.998
				100%	100%	40.09	39.42	0.0273	0.9971
Scenery	77	22	3.63	40%	40%	44.67	43.91	0.0419	0.9991
				100%	100%	40.72	39.94	0.1076	0.9983
Tulip	18	78	5.22	40%	40%	43.05	42.91	0.014	0.9978
				100%	100%	38.08	38.91	0.034	0.9891
Hill	95	4	3.09	40%	40%	46.15	44.79	0.0307	0.9986
				100%	100%	42.29	40.88	0.0822	0.9964

One of the subjective attribute of visual perception is Brightness. Although it is a color appearance parameter of color appearance models, treated differently from color and HVS is much more sensitive to changes in brightness than to changes in color. The brightness of an object is sensed through eye approximately logarithmically over a moderate range. The proposed method uses this characteristic of HVS for selecting the secure region for data embedding.

The famous mathematicians Weber–Fechner introduce laws on human perception in the field of psychophysics. The Fechner's law state that the “Perceived brightness is proportional to logarithm of the actual intensity measured with an accurate nonhuman instrument.” Modern researchers have attempted to incorporate such perceptual effects into mathematical models of vision. Therefore it is clear that the HVS is very much sensitive with the brighter portion of the image; so any change in brighter region due to embedding causes perceivable change in the resulted ‘stego-image’. The perceived brightness is also depends on the intensities of neighbors pixels. The proposed method uses HSV model and the wavelet fusion operation for distinguishing Brighter and Non-Brighter region.

The HVS depends on three different independent attributes of HSV model – Hue, Saturation and Value. Among these the Saturation and Hue is responsible for brightness. The method first converts the color RGB image into HSV image. Then consider S and V component and perform fusion among them. The Brighter and Non-Brighter region is now segregated from this fused image based on some threshold. The threshold selection phase initially selects two thresholds – upper and lower based on statistical analysis and Weber Constant. The final threshold is calculated based these two thresholds and the message length. Embedding of secret data is done on both the region but in different capacity using the proposed method. The target bits are embedded in those pixel region which are fully belongs to its corresponding region with their 8 neighbours. The boundary pixels are not considered for proper extraction of target data at the receiver side. Before embedding secret data is compressed based on the method and then two bits of target data is embedded in each color channel (i.e. one character) of bright region whereas four bits of target data in color channel (i.e. two character) of non-bright region. The proposed method helps in increase capacity with high robustness by maintaining imperceptibility. The result and analyses are shown in Figure 3,Figure 4, Table 2 and Table 3.

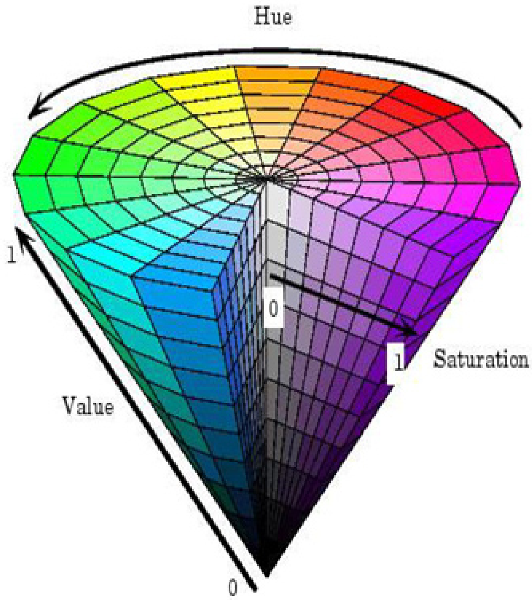
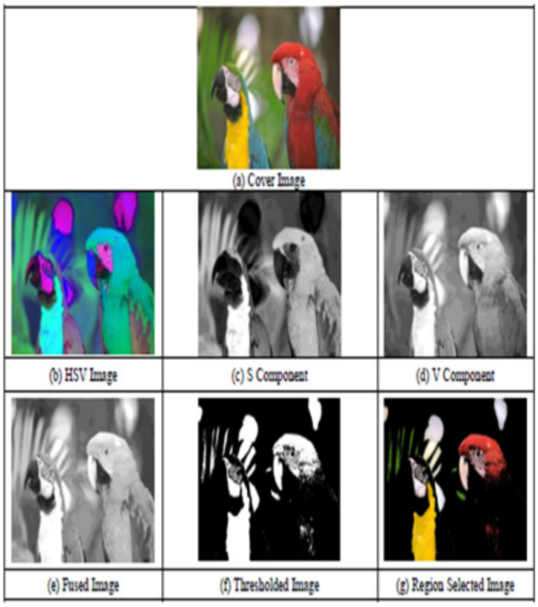


Fig. 3: HSV Model


(a) Cover Image

(b) HSV Image

(c) S Component

(d) V Component

(e) Fused Image

(f) Thresholded Image

(g) Region Selected Image

Figure 4 (a) Cover Image. (b) – (g) the steps for the selection of brightness Region

Table 2: Sample Results

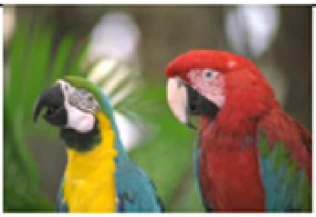
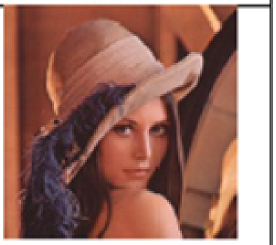
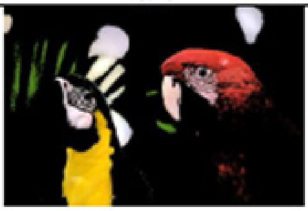
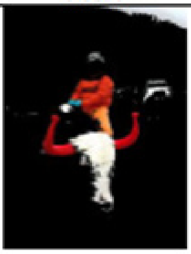
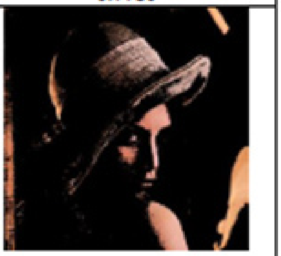
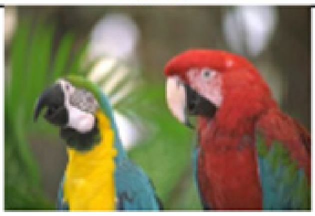
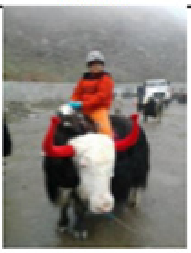
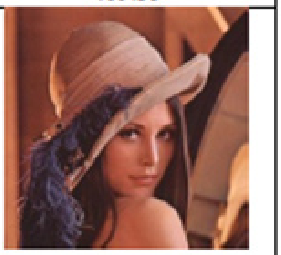
Size	512 × 768	320 × 426	512 × 512
Cover Images			
Threshold	0.76	0.8250	0.7780
Selected Region			
Capacity (Char)	454987	242838	466438
Stego Images			

Table 3: Performance Analysis based on PSNR, SSIM and Capacity

Image	Image Plan	PSNR	SSIM	Embading Capacity (Char)	BPP
Lena(512-512)	Red	35.38	0.9924	466438	11.67
	Green	35.49			
	Blue	35.24			
Baboon(512-512)	Red	36.86	0.9904	329238	10.67
	Green	36.87			
	Blue	36.43			
Bird(512-512)	Red	36.41	0.9921	454987	11.21
	Green	36.47			
	Blue	36.32			
Girl(320-426)	Red	36.19	0.9912	242838	11.43
	Green	36.32			
	Blue	36.22			

Conclusions

The paper proposed with the solution of low capacity issue in standard LSB technique by hiding multiple bits in pixels/samples. The problem of low robustness is solved by embedding data at the higher LSB layer of both image and audio. The techniques may become more robust by considering multiple bit-planes randomly for embedding target data and also perform embedding in virtual bit-planes. The imperceptibility as well as the robustness of steganography techniques are increased by embedding multiple bits in a particular region selected either based on some image attributes or by Human Visual Perception.

Acknowledgement

We are thankful to Techno India Ltd., India, for giving us facilities for developing the proposed method.

Conflict of Interest

There is no conflict of interest.

Funding Agency

Techno India Ltd., India

References

1 X. Shu, J. Zhang, D. D. Yao and W. C. Feng, “Fast Detection of Transformed Data Leaks”, *IEEE Transactions on Information Forensics and Security*, vol. **11**, 2016, pp. 528-542.

2 M. Bergman, “It’s Hard to Get Good (Security) Help These Days”, *IEEE Consumer Electronics Magazine*, Vol. **5**, No. 3, 2016, pp. 132- 133.

3 T. Jamil, “Steganography: The art of hiding information is plain sight”, *IEEE Potentials*, Vol. **18**, No. 01, 1999, pp. 10-12.

4 A. Martin, G. Sapiro and G. Seroussi, “Is image steganography natural?”, *IEEE Transactions on Image Processing*, Vol. **14**, No. 12, 2005, pp. 2040 – 2050.

5 H. B. Kekre, A. Athawale, S. Rao and U. Athawale, “Information Hiding in Audio Signals”, *International Journal of Computer Applications*, Vol. **7**, No. 9, 2010, pp. 14-19.

6 P. N. Basu and T. Bhowmik, “On Embedding of Text in Audio – A case of Steganography”, in proc. of IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.

7 T. Pevny, T. Filler and P. Bas, “Using High-Dimensional Image Models to Perform Highly Undetectable Steganography”, Information Hiding, *Springer*, LNCS, Chapter 20, Vol. **6387**, 2010, pp. 161-177.

8 B. C. Nguyen, S. M. Yoon and H. K. Lee, “Multi Bit Plane Image Steganography”, International Workshop on Digital Watermarking (IWDW 2006), *Lecture Notes in Computer Science*, Vol. **4283**, 2006, pp. 61–70.

9 W. C. Kuo, S. H. Kuo and L. C. Wu, “Multi-Bit Data Hiding Scheme for Compressing Secret Messages”, *Applied Sciences Journal*, Vol. **5**, No. 4, 2015, pp. 1033-1049.