IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

Study of Information Hiding in Images Using Steganography Techniques

Vijay J. Bodke, Priyanka N. Mahale, Gaurav V. Barde, Bhushan S. Chaudhary
K. V. N. Naik Polytechnic, Nashik, Maharashtra

Abstract: *Modernization of technology and having fast Internet make information to allocate over the world easily and economically. This is made people to worry about their secrecy and works. Steganography is a technique that prevents unauthorized users to have access to the important data. The steganography and digital watermarking provide methods that users can hide and mix their information within other information that make them difficult to know by attackers. In this paper, we study some methods of steganography and digital watermarking in both spatial and frequency domains. Also, we explain types of host documents and we focused on types of images.*

Keywords: Steganography, Digital Watermark.

I. INTRODUCTION

The Internet is a modernization technology that has become one of the most important events in modern world history [1]. It contains huge amounts of information in different fields. People who have a computer can get information that related to their fields without any difficulty [8]. As a result, each user who has an internet linking can read up-to-date news on the Internet, watch movies, get books, contact universities, purchase goods, etc [11]. Digital multimedia is data that can allocate easily over the Internet, making many copies of this data, breaking the intellectual property (IP) rights by authorized users more than ever. Thus, owners of those data are thinking for new technologies that promise to protect their rights [3; 5; 7].

Due to the fast invention of software programming on the Internet in the past two years, there has been increasing interest in ways of hiding information in other information [12]. Many techniques are available to prevent unauthorized users from copying information without owner permission [30; 34]. Two of these methods are cryptography and steganography [21; 22]. Cryptography is a rule or protocol between transmitter and receiver using some encryption keys to understand each other. Those encryption keys can be private (the user can make one) or public. Unauthorized users can see the coded information without understanding or being able to read it. The second method is steganography, which is embedded information which does not appear to users [23].

II. STEGANOGRAPHY

Steganography comes from the combination of the Greek words Stegano means sealed and Graphy mentioning to writing which means secret writing. Steganography is the method of hiding secret data within a normal, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganographycan be combined with encryption as an extra step for hiding or protecting data. Steganography is a very old technique of embedding personal information into other data by using some rules and techniques [23]. As a result, unauthorized users are not able to see and recognize the embedded information. Steganography is managing a secret path for sending information invisibly.

Figure1 shows two general directions of steganography: protection against detection and protection against removal [24]. Protection against detection uses some ways to embed information invisibly that does not degrade the quality of the original data. Protection against removal supposes that the method should be able to resist to common digital signal processing and noises. Removing the hidden data will definitely reduce the object's quality and its performance will not be functional [26; 27].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

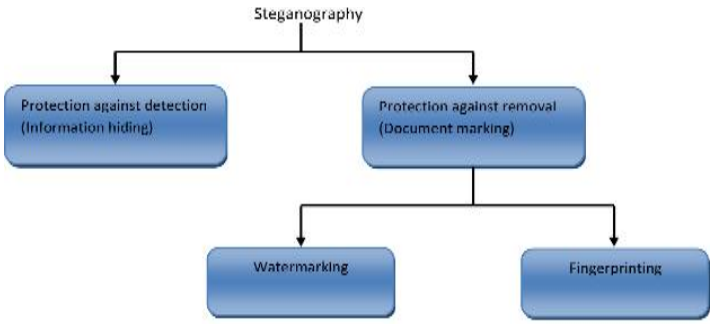

FIGURE 1: Steganography Types

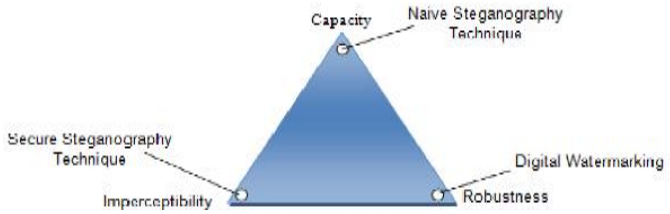

Figure1. Direction within steganography

III. LITERATURE SURVEY

In this paper they stated that result obtained from association rule of a priori algorithm more relationship between accident and crime factors.

DIGITAL WATERMARKING

Digital watermarking is one of the most widely used applications for steganography technique. Digital watermarking is the process of inserting invisible information (a signal) into a component or digital transmitted data which can be detected by a computer algorithm to prove the authenticity and integrity of the component or the transmitted data. Watermarking hides information in a digital signal. It is often unchangeable with text, audio, pictures, or video, for use as copy protection. So, the secret information would mix with the original signal. For example, if the signal is copied, then the information is also carried in the copy [4].

Applications

There are many applications in which digital watermarking can be used. Digital watermarking applications are important which is the requirements of digital are based on them. Applications are such as copy prevention or control, fingerprinting, broadcast monitoring, identification card security, Fraud and tamper detection, data authentication, ownership assertion, and medical applications. Some of those are listed below [42]:

Copy Protection: Called as copy control, to prevent unauthorized users to have making illegal duplicate copies of copyrighted content.

Owner Identification: It is the same as copyright protection, to set up ownership of the content.

Content Authentication: To discover the modifications of the content, as a mark of incorrect authentication.

Fingerprinting: Sometimes described as tracking of transaction or tracking of traitor, to find back distribution of the content and illegal duplication.

Broadcast Monitoring: Used in entertainment and for advertisements and in many industries. The purpose is that to monitor data that have to be broadcasted as contracted and by the authorized user.

Medical Applications: It is very important in medical fields also called as invertible watermarking; it contents both confidentiality and authentication in a reversible manner without having to affect the medical image in any side.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

Classification of Digital Watermarking

There are two kinds of digital watermarking: seen and invisible. In a seen watermarking, facts are seen in the photo or video. The statistics is a text message or organization brand which acknowledges the proprietor of the media. Most tv channels have emblems that point out that the statistics on the unique channel is protected. Nobody is allowed to use this information barring permission from the channel that owns the data. The brand capacity a seen watermark that can be brought [40]. An invisible watermarking is statistics introduced to a digital multimedia object such as a text, audio, image, or video. An object that incorporates an "invisible watermark" have to seem like the unique object. One of the most vital functions of an "invisible watermark" is copyright protection. It is beneficial as a way of recognizing the author, creator, owner, and approved customer of a file or records [35].

Explanation of Images:

As a rely of fact, a pc manipulates photos as a crew of photograph factors referred to as pixels. Each pixel represents a movement of binary numbers that specific the pixel's depth or shade [40]. According to the color, snap shots can be categorized into two types of images. One is a grayscale image, in which every pixel has eight bits (1 byte) and the 2d is coloration image, in which every pixel has 24 bits (3 bytes). The eight - bit photo has 256 exceptional grey palettes (28=256). This kind of photograph will be displayed as a black-and-white image (0 refers to black and 255 is white). A 24-bit picture consists of three essential colors: "red, green, and blue" (RGB); every pixel is represented through three bytes. Each byte refers to the depth of the three foremost colorings RGB, respectively. This kind of photo has proper quality, and the wide variety of palettes is greater than sixteen million (224) distinctive shade [31].

According to extensions, pics are divided into many sorts such as JPEG (Joint Photographic Experts), BMP (Bitmap), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), TIFF (Tagged Image File Format), and etc. Most of these extensions use RGB structure to exhibit depth of pixel color. The internet web page programming such as Hypertext Markup Language (HTML) makes use of RGB, the place every two hexadecimal digits characterize one essential color. This ability every pixel has six hexadecimal digits. For example, the coloration yellow can be created via a full quantity of purple coloration (decimal 255, hex FF); the full quantity of green, the pixel's cost will be "#FFFF00" in the hexadecimal machine wide variety [28; 31]. Images are of one-of-a-kind sizes, which rely definitely on the variety of pixels and additionally on the range of bits in every pixel. The measurement of an 8-bit grey picture consists of decision 320 via 240 pixels which is equal to seventy-five Kilobytes (320*240 bytes), whilst the dimension of a photograph with a full shade (24-bit RGB) is going to be 225 Kilobytes [4; 14; 41]. It is indispensable to decrease picture file sizes when transmitting by way of the internet. For this reason, many compression techniques have been developed over current years. The two most famous sorts of compression are lossy and lossless compression, which are extensively used in picture processing. Compression tactics are mainly beneficial in BMP, GIF, and JPEG file photograph sorts [6;14]. Lossy compression scheme makesof through JPEG pics this method attempts to extend the file close to the measurement of unique file [43].

On the different hand, lossless compression is a scheme that makes use of to rebuild the authentic picture with the aid of making use of some software. GIF and 8-bit BMP are two kinds of pictures which use for this scheme [25; 37].

Watermarking Techniques

Spatial Domain Watermarking

There are many algorithms the utilization of real data, such as video, image, audio, and text, to hide specific facts like emblems or private signatures in a spatial domain. In distinctive words, if the special documents is an image, processing would be into the pixel values barring altering the records into some different domain. The widest and best method in spatial location is Least Significant Bit (LSB), which is altering the first bit in each and every pixel by means of the use of statistics that intends to conceal [13].

Least Significant Bit Watermarking

LSB is the one of the oldest and easiest algorithms that lets in customers to conceal their statistics the use of spatial area [16; 38]. The human eye can't understand the distinction that happens in the two first bits in every pixel. In different words, the trade in the least tremendous bit does now not have an effect on the image's quality. 24-bit pictures have

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

three LSB due to the fact every RGB channel has its personal LSB [15; 29]. This gives customers with greater storage capability to embed the statistics that is imperative to hide. For example, two pixels of an RGB picture colour will grant six bits for watermarking. To encode a message (100111) in RGB picture wants two LSB pixels [13; 31].
RGB Pixel 1 (R: 00010101 G: 11001100 B: 11101100)
RGB Pixel2 (R: 11011111 G: 00010001 B: 11001001)
To conceal the identical message (100111) in a gray-scale photo six LSB pixels are needed.
Pixel1: 10010101 Pixel2: 00001100 Pixel3: 11001000
Pixel4: 10011111 Pixel5: 00010001 Pixel6: 11001011

Frequency Domain Watermarking

This is additionally referred to as seriously change domain, due to the fact the unique facts modifications from spatial to frequency domain. The most frequent frequency strategies are Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation (DWT), and Discrete Cosine Transformation (DCT). For example, an 8-bit picture with a 256 by way of 256 decision can be changed into frequency watermarking the use of DWT. The end result of this processing would be 4 small images, every of them with a 128 through 128 resolutions. Moreover, 4 pictures will have distinctive frequency degrees from low to excessive due to the fact every of them has extraordinary coefficients for others. The primary benefit of the usage of frequency area watermarking is that it is strong for many sorts of sign manipulations when sending information by the Internet. Also, it resists of many noises that assault embedded facts [2; 13; 31].

Discrete Wavelet Transform

It is a device to seriously change the sign or records from one area which is a spatial to any other area which is a frequency. In the frequency area the sign splits into the two 1/2 one of them is excessive frequency and every other is low frequency. Then every of them is going to divide once more into excessive and low frequency that 4 distinctive components of sign [10]. Four components or sub bands of decomposed sign are LL, LH, HL and HH frequencies which are low-low, low-high, high-low and high-high frequencies [10; 29]. Low frequency is the identical of unique signal and different components are greater small print of sign they are now not genuine records as unique one, so we can trade or cast off relies upon on the method that we using.
The reconstruction manner is the contrary of decomposition procedure that ability the 4 bands of divided records have to be blended once more to get better the unique data. Sometimes we do greater than one degree of decomposition relies upon on the algorithm that we use. Low-low frequency band will be used in case we do 2nd decomposition. In case of reconstruction the final degree of decomposition will used first which is specific contrary route [42].

Discrete Cosine Transform

In this device the records will divide into some blocks frequently eight by means of eight or sixteen by using sixteen blocks. Then, making use of a discrete cosine radically change on every block will convert the sign into high, center and low frequencies. Low frequency is very shut to authentic records whilst the center and excessive frequencies are greater small print of the data. We can use the small print frequencies as a host statistic to cover some vital secret on it or we can get rid of these small print frequencies to minimize the dimension of the signal. The reconstruction system is rebuilding the sign in contrary way its ability combining all frequencies high, center and low into single sign [32].

Embedding and Detection Processes

In embedding process, the invulnerable facts which known as the brand will be embedded into the host facts every so often name cowl information and ship to the destination. User can use many secret keys; in general, we can divide into two types. First, symmetric key which each sender and receiver have the equal key for encryption and decryption data. Second, uneven key each transmitter and receiver use extraordinary sorts of keys. Watermarked statistics is the records that has to be dispatched to vacation spot which consists of mixing logo, cowl and key statistics which appears to all people that is one piece of information [39]. Figure4 indicates embedding process.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

In detection process, when the watermarked information reaches to the vacation spot as one piece of information

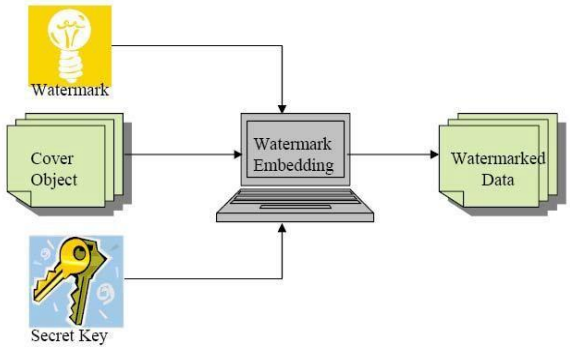

Figure4. Watermark Embedding Process

which in truth it is a crew of blended data. The emblem facts will be extracted from the blended statistics by means of the use of one kind of key. Splitting of these three alerts desires to use one of strategies in each spatial and frequency domain. The extraction technique relies upon on the kind of the algorithm that used and the fine of recovered alerts is unique from the usage of one algorithm to others. Also, the range of decomposition tiers that used in embedding system influences without delay to the excellent of the facts that have been dispatched it by using person which is the usage of the identical range of reconstructions ranges [36].

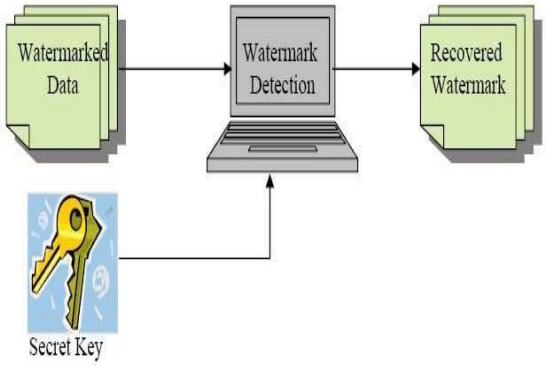

Figure5 suggests detection process

IV. CONCLUSION

Although there are many blessings of the internet, it has additionally opened a new way for invasion of our privateness and mental property by using hackers and unauthorized users. Many methods have been invented on the grounds that these issues appeared. One beneficial method to guard facts by using the web is steganography. Digital watermarking is one of the famous functions for steganography. Users can cover vital data inside aphoto with the aid of the usage of an invisible watermark when they transmit data. Moreover, a seen watermark can be used in many functions such as author, creator, and document. Images have some unimportant areas the human visible device can't understand through changing these areas with different information. A consumer can exchange the least big bit in every pixel with his/her very own statistics barring the nice of a photo being decreased. Also, this alteration does now not have an effect on the depth of the color.

ACKNOWLEDGEMENT

We would like to thank Mrs. D.R. Thakare, our Guide, Mrs.G.R. Jagtap HOD and our Principal, Mr.S.R. Upasani for their support and guidance in completing our paper. It was a great learning experience.

I would like to take this opportunity to express my gratitude to all of my group members AkshadaKhairnar Shravani Modak, Sanjana Shejwalkar. This paper would not have been successful without their cooperation and inputs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

REFERENCES

[1] (2010, 25-27 June 2010). Adaptive steganography scheme using more surrounding pixels. Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on.

[2] Ahmed, A. M., & Day, D. D. (2004). Applications of the naturalness preserving transform to image watermarking and data hiding. Digital Signal Processing, 14(6), 531-549. doi: 10.1016/j.dsp.2004.08.002

[3] Al-Hunaity, M. F., El-Emary, I. M., & Najim, S. A. (2007). Colored digital image watermarking using the wavelet technique. [Article]. American Journal of Applied Sciences, 4(9), 658+.

[4] Al-Otum, H. M., & Samara, N. A. (2010). A robust blind color image watermarking based on wavelet-tree bit host difference selection. Signal Processing, 90(8), 2498-2512. doi: 10.1016/j.sigpro.2010.02.017

[5] Alturki, F., &Mersereau, R. (2001, Apr 2001). A novel approach for increasing security and data embedding capacity in images for data hiding applications. Paper presented at the Information Technology: Coding and Computing, 2001. Proceedings. International Conference on.

[6] Amat, P., Puech, W., Druon, S., &Pedeboy, J. P. (2010). Lossless 3D steganography based on MST and connectivity modification. Signal Processing: Image Communication, 25(6), 400-412. doi: 10.1016/j.image.2010.05.002.

[7] Awwad, W. F., Mansour, R. F., & Mohammed, A. A. (2012). A robust method to detect hidden data from digital images. [Report]. Journal of Information Security, 3(2).

[8] Babu, K. S., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. (2008, 19- 21 Nov. 2008). Authentication of secret information in image Steganography. Paper presented at the TENCON 2008 - 2008 IEEE Region 10 Conference.

[9] Bailey, K., & Francis, M. (2008). Managing information flows for improved value chain performance.International Journal of Production Economics, 111, 2-12.

[10] Chandra, M., & Pandey, S. (2010, 1-3 Aug. 2010). A DWT domain visible watermarking technique for digital images. Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On.

[11] Chang, C.-C., Chen, W.-J., & Le, T. H. N. (2010). High payload steganography mechanism using hybrid edge detector. [Report]. Expert Systems with Applications, 37(4), 3292+.

[12] Chang, C.-C., Chuang, J.-C., & Lin, P.-Y. (2010). A grayscale image steganography based upon discrete cosine transformation. [Technical report]. Journal of Digital Information Management, 8(2), 88+.

[13] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727-752. doi: 10.1016/j.sigpro.2009.08.010

[14] Chen, W.-Y. (2007). Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. Applied Mathematics and Computation, 185(1), 432-448. doi: 10.1016/j.amc.2006.07.041

[15] Chin-Chen, C., & Hsien-Wen, T. (2009, 4-6 June 2009). Data Hiding in Images by Hybrid LSB Substitution. Paper presented at the Multimedia and Ubiquitous Engineering, 2009. MUE '09. Third International Conference on.

[16] Ching-Sheng, H., & Shu-Fen, T. (2010, 26-28 Feb. 2010). Finding Optimal LSB Substitution Using Ant Colony Optimization Algorithm. Paper presented at the Communication Software and Networks, 2010. ICCSN '10. Second International Conference on.

[17] El-Emam, N. N. (2007). Hiding a large amount of data with high security using steganography algorithm. [Article]. Journal of Computer Science, 3(4), 223+.

[18] Farshchi, S. M. R., &Toosizadeh, S. (2011). High secure communication using chaotic double compression steganography technique. [Report]. International Journal of Research and Reviews in Computer Science, 527+.

[19] Hedieh, S., &Jamzad, M. (2008, 8-11 July 2008). Cover Selection Steganography Method Based on Similarity of Image Blocks. Paper presented at the Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

[20] Hung-Min, S., King-Hang, W., Chih-Cheng, L., &Yih-Sien, K. (2007, Oct. 30 2007-Nov. 2 2007). A LSB substitution compatible steganography. Paper presented at the TENCON 2007 - 2007 IEEE Region 10 Conference.
[21] Husainy, M. A. F. A. (2009). Image steganography by mapping pixels to letters. [Report]. Journal of Computer Science, 5(1), 33+.
[22] Ibrahim, B., Jabri, R., &Zoubi, H. A. (2009). Information hiding: a generic approach. [Technical report].Journal of Computer Science, 5(12), 933+.
[23] Jin-Suk, K., Yonghee, Y., & Mee Young, S. (2007, 7-9 Nov. 2007). Steganography using block-based adaptive threshold. Paper presented at the computer and information sciences, 2007. iscis 2007. 22nd international symposium on.
[24] Li, B., Biswas, S., &Blasch, E. P. (2007, 9-12 July 2007). An estimation approach to extract multimedia information in distributed steganographic images. Paper presented at the Information Fusion, 2007 10th International Conference on.
[25] Li, L.-d., Guo, B.-l., & Guo, L. (2008). Rotation, scaling and translation invariant image watermarking using feature points. The Journal of China Universities of Posts and Telecommunications, 15(2), 82-87. doi: 10.1016/s1005-8885(08)60089-8
[26] Martin, A., Sapiro, G., & Seroussi, G. (2005). Is image steganography natural? Image Processing, IEEE Transactions on, 14(12), 2040-2050. doi: 10.1109/tip.2005.859370
[27] Marvel, L. M., Retter, C. T., &Boncelet, C. G., Jr. (1998, 4-7 Oct 1998). Hiding information in images.Paper presented at the Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on.
[28] McBride, B. T., Peterson, G. L., & Gustafson, S. C. (2005). A new blind method for detecting novel steganography. Digital Investigation, 2(1), 50-70. doi: 10.1016/j.diin.2005.01.003
[29] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2011). The quality evaluation of image recovery attack for visible watermarking algorithms. Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.
[30] Neeta, D., Snehal, K., & Jacobs, D. (2007, 6-6 Dec. 2006). Implementation of LSB Steganography and Its Evaluation for Various Bits. Paper presented at the Digital Information Management, 2006 1st International Conference on.
[31] Popa, R. (1998). An analysis of steganographic techniques. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.
[32] Rongsheng, X., Keshuo, W., & Shunzhi, Z. (2007, 16-18 April 2007). An Improved Semi-fragile Digital Watermarking Scheme for Image Authentication. Paper presented at the Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on.
[33] Sarg, S. (2008). Gravito-inertial Propulsion Effect Predicted by the BSM. Supergravitation Unified Theory.
[34] Shaohui, L., Hongxun, Y., & Wen, G. (2004, 5-7 April 2004). Steganalysis of data hiding techniques in wavelet domain. Paper presented at the Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on.
[35] Su, J. K., Hartung, F., &Girod, B. (1998). Digital watermarking of text, image, and video documents.Computers & Graphics, 22(6), 687-695. doi: 10.1016/s0097-8493(98)00089-2
[36] Subbarayan, S., & Karthick Ramanathan, S. (2009, 28-30 Dec. 2009). Effective Watermarking of Digital Audio and Image Using Matlab Technique. Paper presented at the Machine Vision, 2009. ICMV '09. Second International Conference on.
[37] Suhail, M. A., Obaidat, M. S., Ipson, S. S., &Sadoun, B. (2003). A comparative study of digital watermarking in JPEG and JPEG 2000 environments. Information Sciences, 151(0), 93-105. doi: 10.1016/s0020-0255(02)00291-8
[38] Suk-Ling, L., Kai-Chi, L., Cheng, L. M., & Chi-Kwong, C. (2006, Aug. 30 2006-Sept. 1 2006). Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing. Paper presented at the Innovative Computing, Information.