© 2020 IJSRST | Volume 5 | Issue 7 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

4th National Conference on Advances in Engineering and Applied Science
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur, Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

# Comparative study on Video Steganography in Spatial and IWT Domain

**Rizwana Ali[1], Nilesh Bodne[2]**

[1]MTech Scholar, Department of Electronics & Communication Engineering., Vidarbha Institute of technology Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Electronics & Communication Engineering, Vidarbha Institute of technology, Nagpur, Maharashtra, India

## ABSTRACT

In this project we are introducing an enhacement of the grey-scale image ADAPTIVE Stegnography system using LSB(LEST SIGNFICANT BIT) to get a security for the personal data and communication. elective strategy to ensure the licensed innovation of computerized pictures. This Project shows a cross breed dazzle Stegnography method planned by joining RDWT with SVD considering an exchange off among impalpability and strength. The technique embedded the hidden information in the spatial domain of the cover image and uses simple (EX-OR Operationbased).Watermark inserting areas are resolved utilizing a changed entropy of the host picture. Watermark installing is utilized by looking at the symmetrical grid is acquired from the cross breed plot RDWT-SVD. In the proposed plan.

Keywords : JPEG2000, RWDT-SVD, LEST SIGNFICANT BIT, Watermark, RDWT-SVD.

## I. INTRODUCTION

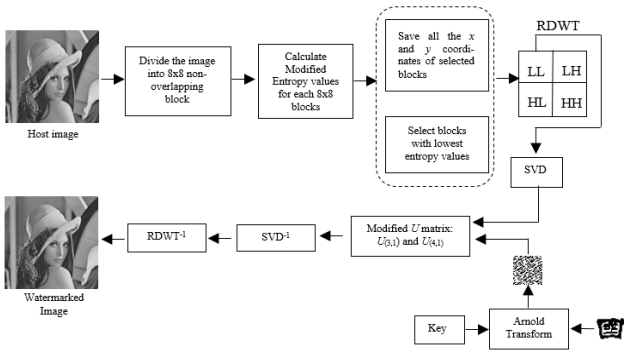
Big data has benefit big popularity and attracting attentions The anticipated idea fuses a model, to be specific, the Features Classification Forest, that extensively enhances the ability of visually impaired Stegnography frameworks without the symptoms of corrupting the physical property and quality, and it will be redone to those Stegnography methods upheld numerical property change or on the other hand a division system. These two courses here imply that a twofold arrangement will be installed by controlling a gathering of the properties of a picture in a methodical way to get a perceived condition inside which each property speaks to exclusively whichever an absolute or opposing approach, that the parallel grouping the absolute approach remains for bit , and furthermore the opposing approach remains for bit 0 will be implanted into the cover image.

Features Classification Forest The main topic utilizes the CRT hypothesis in light of the fact that the adjustment controls and put on the different trigonometric cosine change on an 8 × 8 estimated square. A DC and three AC quantities are picked on the grounds that the inserting zone to install the watermark bit flow.

The topic is included via the protection of JPEG pressure; at the same time, it's to some degree weaker than the fifth idea, which can be appeared inside the investigation area. The second idea applies (SVD) on a 4 × 4 measured square . By moving investigation of the connections of parts inside the U orthogonal lattice, the topic found that

the components set at the subsequent line introductory segment and in this manner the third line starting section are next to each option. Consequently, the watermark bit flow is inserted into the connection of those dual sections by modifying any one in everything about components,For this we will be going to use wavelet transform in our project

- The confidentiality and data integrity are required to protect against unauthorized access.
- This has resulted in an explosive growth of the field of information hiding.
- Moreover, the information hiding technique could be used extensively on applications of, military, commercials, anti-criminal, and so on.
- To protect secret message from being stolen during transmission, there are two ways to solve this problem in general.
- One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully.
- Another way is steganography, steganography literally means covered writing.
- Its goal to hide the fact that communication is taking place.




## II. Image Processing

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image.

Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. Image processing basically includes the following three steps.

- Importing the image with optical scanner or by digital photography
- Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
- Output is the last stage in which result can be altered image or report that is based on image analysis.

## III. Research Methodology/Planning of Work

### Operation

By taking advantage of human perception it is possible to embed data within a file. For example, with audio files frequency masking occurs when two tones with similar frequencies are played at the same time. The listener only hears the louder tone while the quieter one is masked. Similarly, temporal masking occurs when a low-level signal occurs immediately before or after a stronger one as it takes us time to adjust to the hearing the new frequency. This provides a clear point in the file in which to embed the mark.

However many of the formats used for digital media take advantage of compression standards such as MPEG to reduce file sizes by removing the parts which are not perceived by the users. Therefore the mark should be embedded in the perceptually most

significant parts of the file to ensure it survives the compression process.

Clearly embedding the mark in the significant parts of the file will result in a loss of quality since some of the information will be lost. A simple technique involves embedding the mark in the least significant bits which will minimize the distortion. However it also makes it relatively easy to locate and remove the mark. An improvement is to embed the mark only in the least significant bits of randomly chosen data within the file.

In this section a number of different information hiding techniques will be discussed and examined. The media involved vary from images to plain text. While some techniques may be used to hide a certain type of information, in most cases different information can be hidden depending on space restraints.

**Binary File Techniques**

If we are trying to hide some secret information inside a binary file, whether the secret information is a copyright watermark or just simple secret text, we are faced with the problem that any changes to that binary file will cause the execution of it to alter. Just adding one single instruction will cause the executing to be different and therefore the program may not function properly and may crash the system.

You may wonder why people would want to embed information inside binary files, since there are so many other types of data format we can embed information in. The main reason for this is people want to protect their copyright inside a binary program. Of course there are other means of protecting copyright in software, such as serial keys, but if you did a search on the Internet, key generators for common programs are widely available and therefore using serial keys alone may not be enough to protect the binary file's copyright. One method for embedding a watermark in a binary file works as follows. First, let's look at the following lines of code that have been extracted from a binary file

A New Stegnography idea is projected that would impressively enhance present day Stegnography practices. This idea endeavors the highlights of minor images of watermarks of the standard image. This will guide us to maintain secrete content and images in the social media.

This will safeguard us from unwanted hackers. Method of Analysis: To make connection methodology and Similar irrelevant images through fuzzy rules are grouped or might be produced using the host image to simulate an extracted watermark.

This technique, as the feature classification, forest, can do dazzle withdrawal and variable to any Stegnography topic utilizing a quantization-based module. In addition, a greater extent, a watermark is acknowledged while an incompatible influence on the physical property of the cover image. Findings: The tests show the profitable re-enactment of watermarks and furthermore the application to surprising Stegnography plans. One among them features classification, forest marginally balanced from a connection to especially opposing JPEG pressure, and furthermore, the authors demonstrate local benefits of the SVD adjustment method to oppose very surprising image

Due to the rapid and massive development of multimedia and the widespread use of the internet, there is a need for efficient, powerful and effective techniques to protect information. Different Stegnography techniques have been developed in spatial and transform domain methods, however, in recent years; the Stegnography techniques based on transform domain are developed to provide better robustness and imperceptibility [1].

Digital Image Stegnography techniques classified as private, semi private and public Stegnography techniques. In private Stegnography technique the

knowledge of cover image and secret key required to recover the embedded watermark from the watermarked image. In semi-private or semi blind Stegnography technique both the secrete key and the watermark required to extract the inserted watermark. In blind or public Stegnography technique only the secrete key is enough to extract the watermark [2]. Private Stegnography techniques have high robustness than the other two techniques. But the drawback of private Stegnography techniques is that they require original information to extract the watermark [31]. The main requirements of any Stegnography technique include robustness, visibility, and capacity. Robustness is the strength of the watermark so that it can withstand different image processing attacks such as cropping, rotation and compression, etc. Visibility of the watermark related to imperceptibility so that the appearance of the watermarked image may not be degraded by the presence of the watermark. The capacity of the watermark defined as the amount of data carried by it. 2 The technique of digital image Stegnography is used to embed copyright information into multimedia content. Generation of watermark, watermark insertion, detection of watermark and attacks on watermarked image are the different steps in digital image Stegnography [5], [6]. There are four essential factors which include robustness; imperceptibility, capacity, and blindness used to determine the quality of the watermarked image. The robustness of the watermark is tested against attacks like salt&pepper noise, Gaussian noise, JPEG compression, JPEG 2000 compression, median filtering, average filtering, cropping, and rotation [31]. If the presence of the watermark is not destroying the imperceptibility of the cover image, then the technique is said to be more imperceptible. The blind Stegnography technique cannot require the cover image to detect the watermark. The non-blind Stegnography technique requires the original image to detect and extract the watermark. If the secret key and watermark bit sequence are required to detect the presence of the watermark, then the technique is referred to as semi-blind Stegnography.

The Stegnography techniques classified as spatial domain and transform domain techniques based on the domain of watermark insertion. The texture block coding method, least significant bit insertion method and patch work method are existing methods in the spatial domain [8]. In these techniques the location and luminance of the image pixels are processed directly and the drawback of this method is that the lossy compression can easily destroy these bits [22]. In transform domain methods, special transformations are used to process the coefficients in frequency domain to hide the watermark. Different transform domain methods include “Fast Fourier Transform”, “Discrete Cosine Transform”, “Discrete wavelet transform”, “Curvelet Transform”,

## IV. Conclusion

A digital Stegnography technique is an alternative method to protect the intellectual property of digital images. This paper presents a hybrid blind Stegnography technique formulated by combining RDWT with SVD considering a trade-off between imperceptibility and robustness. Watermark embedding locations are determined using a modified entropy of the host image. Watermark embedding is employed by examining the orthogonal matrix U obtained from the hybrid scheme RDWT-SVD. In the proposed scheme, the watermark image in binary format is scrambled by Arnold chaotic map to provide extra security. Our scheme is tested under different types of signal processing and geometrical attacks. The test results demonstrate that the proposed scheme provides higher robustness and less distortion than other existing schemes in withstanding

JPEG2000 compression, cropping, scaling and other noises.

## V. REFERENCES


[1]. C.S. LU: Multimedia securitystegnography and digital watermaking technique for protection of intellectual property. Artech House ,Inc (2003)

[2]. I.J.COX,J.Kallian,T .Leighton,T Shamoon: Secure spread spectrum watermaking for multimedia .Processing of IEEE Image Processing (1997)

[3]. N.A. Abu, F. Ernawan, N. Suryana, Sahib S, "Image Stegnography using psychovisual threshold over the edge," Information and Communication Technology, ICT-EurAsia, vol. 7804, pp. 519-527, 2013.

[4]. F. Ernawan, "Robust image Stegnography based on psychovisual threshold," Journal of ICT Research and Applications, vol. 10, no. 3, pp. 228-242, 2016.

[5]. F. Ernawan, M.N. Kabir, M. Fadli and Z Mustaffa, "Block-based Tchebichef image Stegnography scheme using psychovisual threshold," International Conference on Science and Technology-Computer (ICST 2016), 2016, pp. 6-10.

[6]. F. Ernawan, M. Ramalingam, A. S. Sadiq, Z. Mustaffa, "An improved imperceptibility and robustness of 4x4 DCT-SVD image Stegnography using modified entropy," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 2-7, pp. 111-116, 2017.

[7]. I.A. Ansari, M Pant, "Multipurpose image Stegnography in the domain of DWT based on SVD and ABC," Pattern Recognition Letters, vol. 94, pp. 228-236, 2017.

[8]. S. Fazli, M. Moeini, "A robust image Stegnography method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," Optik - International Journal for Light and Electron Optics, vol. 127, no. 2, pp. 964-972, 2016.

[9]. I.A. Ansari, M. Pant, C.W. Ahn, "Robust and false positive free Stegnography in IWT domain using SVD and ABC," Engineering Applications of Artificial Intelligence, vol. 49, pp. 114-125, 2016.

[10]. N.M. Makbol, B.E. Khoo, T.H. Rassem, K. Loukhaoukha, "A new reliable optimized image Stegnography scheme based on the integer wavelet transform and singular value decomposition for copyright protection," Information Sciences, vol. 417, pp. 381-400, 2017.

[11]. N.M. Makbol, B.E. Khoo, "Robust blind image Stegnography scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," International Journal of Electronic and Communications (AEÜ), vol. 67, no. 2, pp. 102-112, 2013.

[12]. H.-C. Ling, R.C.-W. Phan, S.-H. Heng, "Comment on robust blind image Stegnography scheme based on redundant discrete wavelet transform and singular value decomposition," International Journal of Electronic and Communications (AEÜ), vol. 67, no. 10, pp. 894-897, 2013.

[13]. N.M. Makbol, B.E. Khoo, T.H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image Stegnography scheme using human visual system characteristics," IET Image Processing, vol. 10, no. 1, pp. 34-52, 2016.

[14]. C.C. Lai, "An improved SVD-based Stegnography scheme using human visual characteristics," Optics Communications, vol. 284, no. 4, pp. 938–944, 2011.

[15]. T.D. Hien, Z. Nakao, Y.-W. Chen, "RDWT domain Stegnography based on independent component analysis extraction," Applied Soft Computing Technologies: The Challenge of Complexity. Advances in Soft Computing, 2006, vol. 34, pp. 401-414.

[16]. X.P. Zhang, K. Li, "Comments on an SVD-based Stegnography scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 7, no. 3, pp. 593-594, 2005.

[17]. R. Rykaczewski, "Comments on An SVD-based Stegnography scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 9, no. 2, pp. 421-423, 2007.

[18]. R. Liu, T. Tan, "An SVD-based Stegnography scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121-128, 2002.

[19]. C.C. Lai, C.C. Tsai, "Digital image Stegnography using discrete wavelet transform and singular value decomposition," IEEE Trans. Instrum. Meas., vol. 59, no. 11, pp. 3060-3063, 2010.

[20]. M. Khalili, "DCT-Arnold chaotic based Stegnography using JPEG-YCbCr," Optik - International Journal for Light and Electron Optics, vol. 126, pp. 4367-4371, 2015.

[21]. R. Keshavarzian, A. Aghagolzadeh, "ROI based robust and secure image Stegnography using DWT and Arnold map," International Journal of Electronic and Communications (AEÜ), vol. 70, pp.278-288, 2016.

[22]. M. Khalili, D. Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image Stegnography using Arnold transform map," IET Signal Processing, vol. 7, no. 3, pp. 177–187, 2013.

[23]. R. Zhang, Y. Wang, "Scrambling image watermark algorithm based on DCT and HVS," International Conference on Information Technology and Applications, Nov. 2013, pp. 54–57.