An Alternative LSB Based Video Steganography

Kim Scicluna
Malta College Of Arts, Science And Technology
Institute Of Information and Communication Technology Kordin Street, Rahal Gdid
Email: kim.scicluna.a106280@mcast.edu.mt

***Abstract*—Encryption is a commonly used method of security that can help prevent access to the original contents of a message. Nonetheless, the unauthorised presence of communication between two or more parties can still prove to be a breach of privacy. Such a problem can be overcome with steganography, this being security by obscurity, which hides the presence of a communication channel. This research focuses on the feasibility of an LSB based video steganography technique which uses both the audio and frames as a cover for hiding any secret message. This proposed technique takes advantage of the numerous number of frames and audio samples in a video, instead of utilising just the audio or the frames individually. This gives the possibility of significantly increasing the capacity of secret data that can be embedded in the video. This was tackled by developing two sub-algorithms for audio and image steganography separately, which are based and built upon existing research. Both sub-algorithms were then adapted and combined for a video steganography algorithm. To address the research question, there was an improvement of a video steganography approach utilising both image and audio streams over a video steganography approach which utilises only the audio or frames.**

***Keywords*—Steganography, LSB**

I. Introduction

A. Motivation

No communication could be considered private on the internet. Privacy breaches happen every year, including that of governments exploiting wiretapping laws among other privacy invasion incidents exposed by whistleblowers namely Edward Snowden who said “I don’t want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity or love or friendship is recorded.” Security against these problems often exists in the form of cryptography. However, cryptography does not hide the fact that a communication channel exists between two or more parties. This is where steganography comes in. With digital steganography, covert communication can be established between two or more parties by using innocent looking digital cover media, which secretly hold data embedded inside them. This data can then be extracted only by those who are expecting data to be hidden inside the cover media. This process is known as ‘security by obscurity’.

B. Scope

At present, there is a lack of video steganography algorithms which take advantage of the characteristics of a video, including the numerous amounts of frames in a video and the audio stream of a video. Existing research on video steganography usually deals with either one of the two. For this research, both areas of image and audio steganography were explored.

C. Practical Relevance of Research

An improved video steganography algorithm offers a better and more efficient approach to the area of steganography. Developing optimal sub-algorithms for audio and image steganography was a goal for the research. This was achieved by improving on and adapting existing audio and image steganography algorithms to be used in a video.

II. Literature Review

Steganography is the art of information hiding, a variant of cryptography, both of which can be used for beneficial or malicious intents. Abdulzahra H. et al. (2014) state, steganography prevents any discovery of a communication channel between two or more parties. Steganography utilises a medium, which could be anything from a handwritten letter, a video, and any digital media. In the case of this research, the cover medium was a video.

A. Using Cryptography with Steganography

Aung and Naing (2014) proposed an image steganography technique that utilises both steganography and AES cryptography. Aung and Naing’s (2014) implementation uses symmetric encryption. Symmetric cryptography uses a secret key to encrypt and decrypt the data, and this secret key is known by all the parties of the communication channel. Chhillar R. S. (2015) also explored the use of combining steganography and cryptography, where they state that the method is a good practice in steganography as it adds a layer of security against unauthorised access. However, they used asymmetric cryptography and LSB steganography. Abikoye O. C. et al.’s (2012) method also incorporated cryptography with audio steganography.

B. Image Steganography

Singh A. and Singh S. J.’s (2014) overview of image steganography provides an insight into different image steganography techniques, all of which can be utilised for video steganography.

C. LSB Based Image Steganography

LSB insertion, which is a SD technique, is the most conventional and straightforward method for embedding data in a cover file. As described by Swain G. and Lenka S. K. (2014), LSB steganography in images is done by hiding the bits in the least significant bit of the RGB channels of an image.

D. Using a PRNG with Steganography

To further protect against unauthorised extraction of the embedded data, Emam M. M. et al. (2016) propose an LSB method based on random pixel selection using a PRNG. This proposed technique works as a SKS technique, as opposed to a PKS technique where a public key is used for embedding, and a separate private key is used for extracting the secret data (Mishra M. et al., 2012). SKS is where the secret key, known only by those part of the covert communication channel, is used to generate a pseudorandom sequence that was used to choose the pixels randomly for the embedding and extracting of the secret data. Manjula G. R. and Danti A. (2015) also propose a hash-based 2-3-3 LSB based algorithm, meaning that 8 bits are stored in a pixel, two being in red, 3 in green and 3 in blue. Such a technique provided better PSNR results compared to the original algorithm.

E. Audio Steganography

The journal of Jayaram P. et al. (2011) goes through different audio steganography techniques. LSB Coding is done like image steganography, where the last bit of an audio sample is changed to represent a bit of the secret message. This is not very robust in audio steganography as it can produce distorted sound. The more bits in an audio sample, the smaller the distortion caused. However, with some enhancement, such a technique can become robust and efficient.

F. LSB Based Audio Steganography

Atoum M. S. et al. (2017) proposed advanced LSB technique that increased security. The authors explain that LSB is weak against intentional and unintentional attempts to extract the secret data. The proposed algorithm is an NKS, meaning no key is used for embedding and extracting the secret payload. This technique had higher PSNR values than a standard LSB technique.

Bahl J. and Ramakishore R. (2015) propose a method using LSB and parity coding. Nosrati M. et al. (2012) write that parity coding separates the signal into regions of samples. The parity bit of the region is compared with the bit to be embedded. If they match, no change is done; otherwise the LSB is flipped. Such a method provides distortion as it is less obtrusive on the signal integrity.

G. Video Steganography

The areas mentioned, audio and image steganography, was used in this study. However, other existing video steganography techniques needed to be taken into consideration when it comes to analysing the quality of the proposed video steganography technique with respect to the cover and payload sizes. Sahu U. and Mitra S.'s (2011) video steganography method, which utilises LSB insertion with random frame selection and pixel position selection, was one of the algorithm that was taken into account during this research.

H. Existing Video Stegangoraphy Tool

As Hernandez-Castro J. and Sloan T. (2015) explain in their paper regarding forensic analysis of video steganography tools, this results in the tools available to the public being outdated and do not reflect the latest technological advances in this field. As Hernandez-Castro J. and Sloan T. (2015) mention a video steganography tool named MSU StegoVideo by Vatolin D., 2007. They managed to develop one of the few video steganography tools available that do decent video steganography. As this technique uses compression, the secret message embedded may not be retrieved with 100% integrity. Wu J. et al. (2010) explain that Vatolin D.'s (2007) implementation is an LSB based algorithm that also works with compression, at the cost of having partial message loss upon extraction.

I. Quality Metrics Used

The paper by Kharrazi M. et al. (2006) also gives some parameters that are usually used to rate imperceptibility. First, the number of modifications done to the cover media show how detectable the stego-video file is. The fewer the changes, the less detectable. Another parameter is the MSE, which is an error metric calculated with the original cover media and the stego-video. Another relevant parameter to video steganography is the structural similarity measure. This provides a quantification of similarity between the cover and stego-media. The final and most commonly used metric that is derived from MSE is the PSNR.

III. Research Methodology

The work was divided into two parts, namely, that of embedding and extracting the secret message. For added security, encryption and decryption was done on the secret message, prior and after embedding and extracting. This research contributes to LSB steganography in an attempt to develop a sound and robust LSB steganography algorithm, while maintaining its reputation as a relatively simple implementation.

A. Encryption And Decryption

The encryption of the secret message was a vital process to increase the security of the proposed video steganography algorithm. Chhillar R. S. (2015) states that encrypting the message before steganography is good practice as it is an extra security feature, which protects against the possibility of unauthorised data extraction from the cover video by steganalysis attacks. AES encryption was used because it is a symmetric algorithm, it is fast and lossless.

B. Pseudo-Random Number Generator

The proposed method functioned using a secret key, where everyone in the covert communication channel knows the shared secret key for where its value is used as a seed for a PRNG, and a secret key for the AES algorithm mentioned previously. This process is illustrated in Figure 1.

The PRNG was used for the distribution of the secret data equally and randomly throughout the frames and audio samples by generating a sequence of pseudo-random numbers that indicate the pixels and samples which contain the secret data, inspired by the research of Emam M. M. et al. (2016).

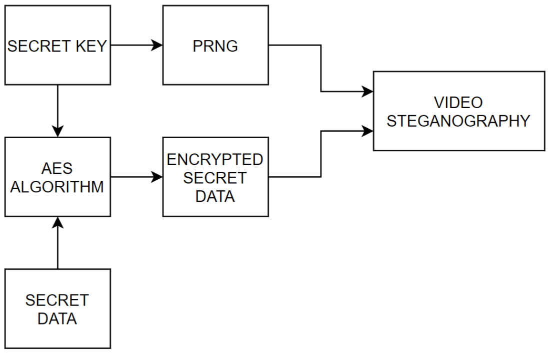

Fig. 1: The use of the secret key

C. Image Steganograpy Sub-Algorithm

The steps of the embedding sub-algorithm are:

1) Get secret data, key and cover image
2) Calculate length of the secret data
3) Generate a pseudo-random sequence of numbers using the key
4) Calculate the bytes per frame by dividing the length by total frames - 1
5) Embed length in first frame using 2-3-3 LSB Embedding
6) Embed the number of bytes found in step 4 in the remaining frames using 2-3-3 LSB Embedding

The steps of the extracting sub-algorithm are:

1) Get the key and stego-image
2) Generate a pseudo-random sequence of numbers using the key
3) Extract length from first frame
4) Calculate the bytes per frame by dividing the length by total frames - 1
5) Extract data in the order of the pseudo-random sequence.

D. Audio Steganography Sub-Algorithm

Aspects from Bahl J. and Ramakishore R.'s (2015) implementation were used. The idea of taking sample regions was adopted. However, the regions taken would have one byte of data, instead of one bit, embedded in them. A region includes thousands of samples, more than enough for the data to fit. The eight bits were inserted pseudo-randomly in LSB of that specific region. This is shown in Figure 2. The steps of the embedding sub-algorithm are:

1) Get secret data, key and cover audio
2) Calculate the length of the secret data
3) Generate a pseudo-random sequence of numbers using the key
4) Embed length in the first 300 bytes of the audio stream using the pseudo-random sequence
5) Calculate the region size per byte by dividing total samples the length
6) Embed each byte in its respective region in random bytes indicated by the pseudo-random sequence

The steps of the extracting sub-algorithm are:

1) Get key and stego-audio
2) Generate a pseudo-random sequence of numbers using the key
3) Extract length from the first 300 bytes using the pseudo-random sequence
4) Calculate the region size per byte
5) Extract each byte from each region using the pseudo-random sequence

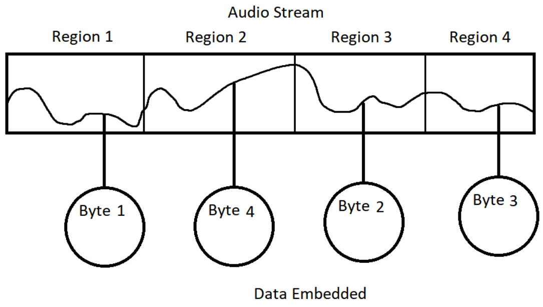

Fig. 2: Bytes randomly embedded in regions of the audio stream

E. Video Steganography Sub-Algorithm

The proposed video steganography technique adopts the mentioned techniques for the audio and frames. The algorithm takes advantage of a large number of audio samples and frames present in a video as opposed to focusing the secret data to be embedded in one hidden frame or audio only.
The steps of the embedding algorithm are:

1) Get key, secret message, distribution ratio and cover video
2) Encrypt secret message
3) Split secret message by distribution ratio
4) Split video in frames and audio
5) Do image steganography on each frame
6) Do audio steganography on audio stream
7) Recompile video

The steps of the extracting algorithm are:

1) Get key and cover video
2) Split video in frames and audio
3) Do image steganography extraction on each frame
4) Do audio steganography extraction on audio stream
5) Rebuild extracted messages
6) Decrypt rebuilt secret message

F. Assumptions Taken

The following is a list of assumptions which were used in this research methodology, mainly regarding the key-agreement protocol to be used between the users in the covert communication channel that utilised the proposed technique.

1) In this research, it is assumed that the users who are communicating have prior knowledge of the single secret key phrase that is used to embed and extract

data. Such issue is usually not tackled in the reviewed literature, and it is a whole separate area of study.

2) Another assumption (and limitation) in this research is that AVI files were used with the algorithm. This is because of the AVIFile Windows library that is used in the development of the prototype, which were used to gather the results needed.
3) If the produced stego-media is compressed with a lossy compression technique, it loses its embedded data. This is also limitation of the research since SD techniques are being used for steganography.

G. Data Gathering And Analysis

A number of stego videos were created with different secret message sizes and different cover media sizes. Mainly, the relationship between these two variables was analysed under different conditions. The metrics used were mainly, Imperceptibility and Payload Size was used.
The analysis of the proposed algorithm was carried out on the whole video to analyse the overall performance of the algorithm but also on the frames and audio separately. The imperceptibility metrics mentioned by Kharrazi M. et al. (2006) were also used.

IV. Results

A. Quality Metrics Used

PSNR is the primary metric used to measure how perceivable the resulting noise caused by the algorithm in the gathered results was, as mentioned by Kharrazi M. et al.'s (2006).

B. Payload Capacity

Image steganography sub-algorithm's payload capacity is calculated by:

$$C_{\text{Image}} = Width \times Height \tag{1}$$

Audio steganography sub-algorithm's payload capacity is calculated by:

$$C_{\text{Audio}} = \lfloor \frac{Subchunk2Size}{8} \rfloor \tag{2}$$

Video steganography algorithm's payload capacity is calculated by:

$$C_{\text{Video}} = ((N-1) \times C_{\text{Image}}) + C_{\text{Audio}} \tag{3}$$

C. The Data Gathering Process

The testing of the video steganography algorithm was split into three stages, being the testing of each individual sub-algorithm and the video steganography algorithm combining both. The image steganography used for the frames of a cover video was tested separately from the audio steganography sub-algorithm used for the audio stream of the video.

D. Testing of the Image Steganography Sub-Algorithm

The first results in Figure 3 highlight PSNR difference between the proposed sub-algorithm and the work of Manjula G.R. and Danti A. (2015) where the same cover media and secret message size were used. The second set of results in Figure 4 highlight PSNR differences between commonly used images for image steganography testing.

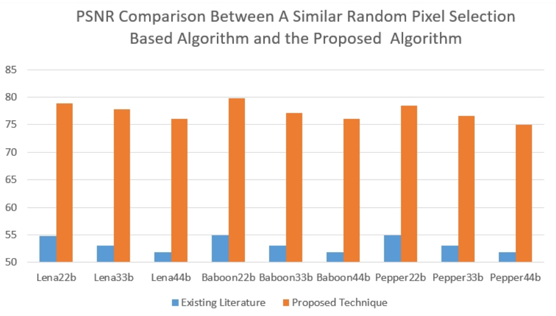

Fig. 3: PSNR comparison between a similar random pixel selection based algorithm and the proposed algorithm

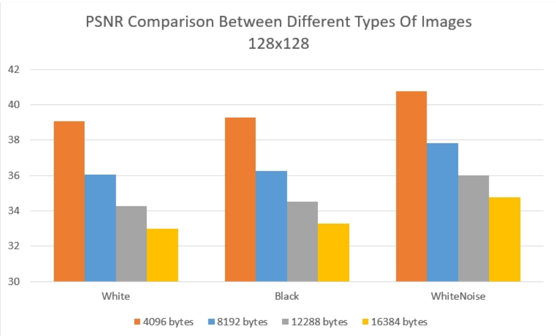

Fig. 4: PSNR comparison between different types of images 128x128

E. Testing of the Audio Steganography Sub-Algorithm

The audio steganography sub-algorithm was tested slightly differently due to the lack of good literature results to compare the obtained results. Having this problem, the algorithm was instead tested under different types of wave files, utilising frequency tones, Gaussian noise, a tone sweep and speech with background noise.
The first test was done on six different frequency tones, complete silence and white Gaussian noise, each being 10 seconds long. This is shown in Figure 5.

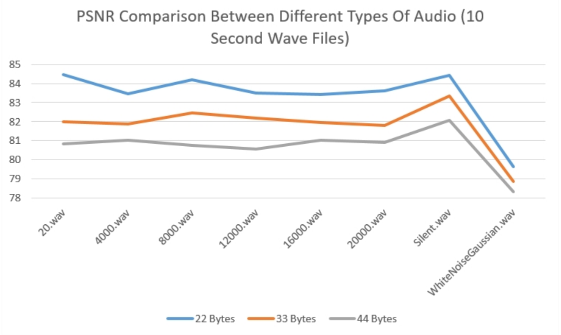

Fig. 5: PSNR comparison between different types of audio

F. *Testing of the Video Steganography Algorithm*

The first test carried out for the video steganography algorithm, shown in Figure 6, tested the different amounts of secret message distribution between the frames and audio streams. The test uses 2048 bytes of secret data. Five different test cases were simulated, each splitting the secret data differently between the frames and audio.

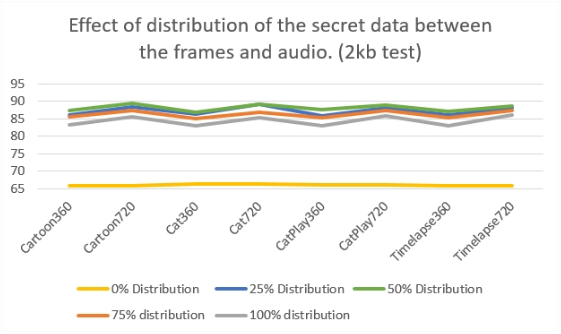

Fig. 6: Effect of distribution of the secret data between the frames and audio. (2kb test)

The following test compares the algorithm with an algorithm from the video steganography tool developed by Vatolin D. (2007). The results gathered are shown in Table I.

Video	**Message Size (Bytes)**	**MSUStegoVideo**	**Proposed Algorithm**
Cartoon	2048	16.3	85.50766
Cat	2048	15.6	85.1124
CatPlay	2048	17.1	85.30766
Timelapse	2048	16.7	85.20305

TABLE I: Comparison between MSUStegoVideo and the proposed algorithm

V. Discussion

In this study, the researcher has investigated the possibility of creating a video steganography algorithm based on the basic LSB technique. This incorporated image and audio steganography techniques inspired by existing literature. Since a digital video file is nothing more than a container for a sequence of images and an audio stream, the main hypotheses regarding the possibility utilising both the video frames and audio streams were first tested in a divide and conquer manner. This was achieved by developing two sub-algorithms involving audio and images separately. Both algorithms developed are based on the most influential aspects of different techniques. On the other hand, the divide and conquer approach allowed for easier testing and performances comparison, by first focusing on both parts separately and then combining them as a whole. This structure is shown in Figure 7.

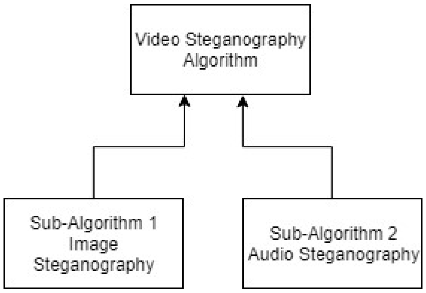
Video Steganography Algorithm
Sub-Algorithm 1 Image Steganography
Sub-Algorithm 2 Audio Steganography

Fig. 7: The structure of the video steganography algorithm

A. *The Algorithm's Efficiency*

By dividing and analysing both audio and image steganography sub-algorithms separately, the efficiency of a video algorithm that utilises image and audio steganography was assessed to help answer the research question. Results indicated that the developed sub-algorithms show that they are efficient enough to be used for a video steganography algorithm. The secret message"s integrity was kept after the extraction process of each test. Ideal video conditions to help to hide the noise caused by the steganography were also researched.

B. *The Distribution Ratio*

When data was embedded in a video's frames and audio stream, there were improved results. The 0% distribution test (all data embedded in the audio stream) shows how poorly the LSB based audio steganography algorithm works when compared to the proposed video algorithm utilising both the frames and audio. The same can be said when a 100% distribution value. The resulting PSNR value was not as low as the audio. However, it was still about 3 dB lower than the proposed method of distributing data between the frames and audio streams. The 25% to 75% distribution values had the best results, coming close to each other, varying by 1 dB to 2 dB. There still was an improvement, albeit a small one, when the secret data was split.

C. *The Payload Capacity*

The proposed video steganography algorithm also increases the payload capacity. Sahu U. and Mitra S.'s (2011) implementation utilises a selection of frames similar to the proposed algorithm. By utilising all the frames and audio stream the average PSNR was kept higher because the overall noise density is lower. The addition of the audio channel further increases the payload capacity.

D. The Perceivability Of The Algorithm

The most perceivable part of the resulting videos of the proposed algorithm was the audio. Even small amounts of data caused audible noise in the audio stream. On the other hand, it is challenging for humans to perceive pixel changes in the frames, especially if the video is of low quality. A possible way to counter this is to use a cover video with noisy audio to mask the audible pops and cracks created by the audio steganography sub-algorithm. While an increase of 3 dB may not seem much between a frames-only video steganography and video-audio steganography, it was still an improvement and could be beneficial when used with the correct cover media, that is, noisy cover media. This can be achieved with pre-processing before any steganography is done on the video, which could be a beneficial improvement upon the proposed algorithm.

VI. Conclusion

The findings obtained proved to be very helpful in answering the hypothesis. An improved video steganography algorithm was developed and showed promising results namely that if both the audio and frames are used, there would be higher PSNR values, causing a lower impact on video quality. Along with this, an increase in message capacity of a video was achieved. The ideal cover media conditions to help camouflage the noise caused by the steganography were also explored.

A. Limitations

The limitations identified in this study are the following:

1) Processing of video steganography took a considerable amount of time.
2) It has been assumed that the single secret key phrase is known by both communicating parties and used to embed and extract data.
3) Only AVI files were used as cover videos.
4) If the produced stego-media is compressed with a lossy compression technique, it will lose its embedded data.
5) Building on limitation 4, compression on the video with the embedded data destroys the integrity of the secret message upon extraction.
6) The limits set by the data types used to implement the algorithm were a limitation. An example of this would be the 2,147,483,647 bit limit that can be embedded inside a single frame or sample region, because of the integer's maximum value.

B. Further Research

Possible further research topics include:

1) Implementing a similar video steganography algorithm that can hold message integrity after compression.
2) Implementing a public key algorithm.
3) Researching the possibility of a relationship between video characteristics (amount of frames, number of samples etc.) and distribution ratio of the secret data to be embedded to obtain optimal PSNR values.
4) Testing against steganalysis attacks.
5) Possible implementation of pre-processing techniques, such as adding noise, to be done prior to the steganography.

References

[1] Abdulzahra, H., Ahmad, R.O.B.I.A.H. and Noor, N.M., 2014. Combining cryptography and steganography for data hiding in images. ACACOS, Applied Computational Science, pp.978-960.

[2] Abikoye, O.C., Adewole, K.S. and Oladipupo, A.J., 2012. Efficient data hiding system using cryptography and steganography.

[3] Atoum, M.S., Alnabhan, M.M. and Habboush, A., 2017. ADVANCED LSB TECHNIQUE FOR AUDIO STENOGRAPHY.

[4] Aung, P.P. and Naing, T.M., 2014. A novel secure combination technique of steganography and cryptography. International Journal of Information Technology, Modeling and Computing (IJITMC), 2(1), pp.55-62.

[5] Bahl, M. and Girdhar, A., 2012. Steganography using the Technique of Orderly Changing of Pixel Components. International Journal of Computer Applications, 58(6).

[6] Chhillar, R.S., 2015. Data Hiding using Advanced LSB with RSA Algorithm. International Journal of Computer Applications, 122(4).

[7] Emam, M.M., Aly, A.A. and Omara, F.A., 2016. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. (IJACSA) International Journal of Advanced Computer Science and Applications, 7(3).

[8] Jayaram, P., Ranganatha, H.R. and Anupama, H.S., 2011. Information hiding using audio steganographya survey. The International Journal of Multimedia & Its Applications (IJMA) Vol, 3, pp.86-96.

[9] Kharrazi, M., Sencar, H.T. and Memon, N., 2006, October. Cover selection for steganographic embedding. In Image Processing, 2006 IEEE International Conference on (pp. 117-120). IEEE.

[10] Manjula, G.R. and Danti, A., 2015. A novel hash based least significant bit (2-3-3) image steganography in spatial domain. arXiv preprint arXiv:1503.03674.

[11] Mishra, M., Mishra, P. and Adhikary, M.C., 2012. Digital image data hiding techniques: A comparative study. arXiv preprint arXiv:1408.3564.

[12] Nosrati, M., Karimi, R. and Hariri, M., 2012. Audio steganography: A survey on recent approaches. world applied programming, 2(3), pp.202-205.

[13] Sahu, M.U. and Mitra, M.S., 2015. A Secure Data Hiding Technique Using Video Steganography. International Journal of Computer Science & Communication Networks, 5(5), pp.348-357.

[14] Singh, A. and Singh, S.J., 2014. An Overview of Image Steganography Techniques. International Journal of Engineering and Computer Science, 3(07).

[15] Sloan, T. and Hernandez-Castro, J., 2015. Forensic analysis of video steganography tools. PeerJ Computer Science, 1, p.e7.

[16] Swain, G. and Lenka, S.K., 2014. Classification of image steganography techniques in spatial domain: a study. International Journal of Computer Science & Engineering Technology, 5(03), pp.219-232.

[17] Dmitriy Vatolin OP. 2007. Msu stegovideo. Available at http://goo.gl/XqiWi1.

[18] Wu, J., Zhang, R., Chen, M. and Niu, X., 2010, April. Steganalysis of msu stego video based on discontinuous coefficient. In Computer Engineering and Technology (ICCET), 2010 2nd International Conference on (Vol. 2, pp. V2-96). IEEE.