

Applying LSB Steganography for Disseminating Academic Testimonials in e-Learning and its Authentication aspects

Soumendu Banerjee^{#1}, Sunil Karforma^{*2}, Akash Nag^{*3}

^{1,3}Research Scholar, Department of Computer Science, The University of Burdwan
Golapbag, Burdwan-713104, West Bengal, India

²Associate Professor, Department of Computer Science, the University of Burdwan
Golapbag, Burdwan-713104, West Bengal, India

Abstract: In the present day scenario, security plays a vital role in e-learning system. In an e-learning system, all kinds of transmissions and communications between the participants of any e-learning system are done via Internet. Since, Internet is publicly accessible; authenticity has a major role to play. Steganography is one of such techniques through which authenticity can be achieved in e-learning. In our proposed system, we have applied Least Significant Bit steganography technique on the color images and also discussed about the compression algorithm. For all the individual applications, we calculate the MSE and PSNR values to check the portability of the proposed system.

Keywords: e-Learning, LSB based steganography, Haar wavelet transform, PackBits compression

I. INTRODUCTION

E-Learning is the application of information and communication technology (ICT), which helps to transmit the educational testimonials between the components of any e-learning system. The main components or participants in an e-learning system are: Administrator or Developer, Teachers and Students or Learners^[1]. One of the main functions of administrator is to provide authentication regarding the transmission of any kind of e-learning documents. Transmitting of documents from developer to students can be of various types, sometimes it may be some alpha numeric characters like unique identification number, user-id, password which are very confidential documents for the students and sometimes it may contain digital images like scan copy of registration certificates, admit cards, mark sheets etc. Here, we can see that all these documents are very essential for the students for their future references. When a student wants to log into their e-learning portal, this user-id and password helps them. So if the hacker can reach this number, they can also use this portal and may cause harmful to the system. In this kind of transmission, to provide authenticity and secrecy, administrators can use LSB based

steganographic approach. Using this technique, when the administrator sends any digitally signed documents to the learner, if the hacker may be able to reach that document and try to tamper that document, and then it can be easily traceable by the learner, which provides authenticity to the learner. Apart from this technique, in this paper, we also have applied a combination of two well known compression algorithms, Haar wavelet transform^[2] and PackBits^[3] algorithms, which may be used by the administrator and it is not mandatory to apply, but may seem helpful for secure transmission mainly in case of transmitting digitally signed digital images. For this digital signing purpose, we have used the improved DSA algorithm for signing our documents^[4].

Steganography is a technique through which sender can conceal the text, image, audio or video within another file, image, audio or video^[5]. The main aim of steganography is to hide information from the outer worlds and image is the main concern in this technique, since a large amount of redundant space is created while storing the images^[6]. This paper is concerned about the transmitting of e-learning testimonials from the administrator to learners. In the proposed model, we have provided two options to the administrator, before sending the documents, the administrators may choose the option of compressing the material or not. These two techniques are explained using the images, shown in annexure (Fig.1 and Fig.2).

In annexure, Fig.1 shows that the administrator of the e-learning institution is sending the secret message may be in text format or as an image, hiding in the cover image to the student. LSB Encoding means the Least Significant Bit technique through which the cover image can hide the secret text from the outer world. After encoding the cover image wrapped with the secret message is known as the stego image. This image will be sent to the learner and learner will decode the secret message from the transmitted stego image. During transmission if the hacker may reach the documents, can't make sense about the hidden text, since it is covered by the cover image.

In annexure, Fig.2 shows the second case, where the administrator will send the documents after applying Haar wavelet transform and PackBit algorithm, if necessary, with the secret image or text. This will reduce the size of the image, but when it will be decoded at the learner’s end, some degradation of the quality of the sending documents is obvious.

In this paper, we have discussed about the transmission of teaching testimonials in two ways: a) either applying without compression algorithm or b) with application of compression algorithm, using the color image as cover image. To achieve secrecy and authenticity regarding transmission, we have used Least Significant Bit algorithm to encode the sending documents. Section II covers the algorithms we have used in our proposed system and section III includes some observations of the applications of our system along with the MSE (Mean Squared Error) and PSNR (Peak Signal - to - Noise Ratio) values. Here PSNR is calculated between the original image and the stego image to measure the quality of the reconstruction. Finally, we conclude in section IV by showing some future scopes.

II. ALGORITHM OF PROPOSED MODEL

In our proposed algorithm, the secret image must be small in size; otherwise, we will not get the appropriate result. On that basis, first the administrators have to choose either they want to apply the compression or not. In the following discussion, for better understanding of our algorithm, we represent the conversion of the original image to steganographic image or stego image by using flowchart, which has been done at the developers’ end.

Flowchart:

The flowchart is shown in annexure, fig.3, which is designed for those cases, where the administrator will use the compression algorithm, but if the administrator doesn’t want to apply the compression, that case will be much easier and will contain less steps. Since, it is easy to understand that which processes will be omitted, so, we are not going to discuss it in detail.

Discussion: The foremost condition of our proposed algorithm is that, the cover image must be in BMP (Windows Bitmap) format, and it must be a color image, which can be decomposed in RGB (red, Green and Blue) channel. The reason behind taking only bitmap images is that in case of JPG or JPEG formats, images are already in compressed form and different compression algorithms are used to make those images compressed. So, when we apply those compressed images, in our proposed system, the output file size will be increased, which

may be a reason to make doubt about the sending document, if the hacker can reach to it, while sending from administrator to student. This increased size is also unjustified for the steganography.

For our secret image, the range of the color value is in between 0 to 255, which can be converted into an 8 bit binary value. In the same way, we retrieve one pixel from the cover image and converted it into RGB channel. For each bit, extracted from the secret image, we take two successive color values from the cover image in binary form for hiding one bit of secret image into cover image. Each octet is divided into two parts: Hiding section and Index section^[7].

1	2	3	4	5	6	1	2
7	8	9	10	11	12	3	4

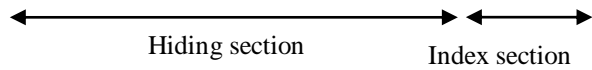


Fig.4: Separation of hiding section and index section

To increase the storing space, we will take 2 octets at a time for hiding one bit of information. For these 2 octets, we will pick up one pixel from the cover image and separate it into 3 channels (RGB). Since, we have required only two channels, we will keep one of these three fixed at a time. For better understanding, let us take an example below:

Let the value (value-s) from the secret image is 36 and after converting it to binary we get $(36)_{10} = (00100100)_2$

For each value-s, we will take one pixel from the cover image and convert it into RGB channel, which will provide 3x8 array and convert it also in binary.

Let $R=(152)_{10}$ then after converting into its equivalent binary $R=(10011000)_2$

Let $G=(211)_{10}$ then after converting into its equivalent binary $G=(11010011)_2$ and

Let $B=(64)_{10}$ and after converting into its equivalent binary $B=(01000000)_2$

1	0	0	1	1	0	0	0
1	1	0	1	0	0	1	1
0	1	0	0	0	0	0	0

Fig.5: Arranging RGB of cover image

For this particular case suppose, the Blue channel is kept unchanged and changes occur in Red and Green channel. The first bit of value-s that is bit-s ‘0’ will be hidden in the [0][1] position and the positions [0][6], [0][7], [1][6 and [1][7] will work as index and store the [0][1] position that is index number $2=(0010)_2$

So after successfully hiding the bit the array of fig 2.3 will be changed as following figure:

1	0	0	1	1	0	0	0
1	1	0	1	0	0	1	0
0	1	0	0	0	0	0	0

Fig.6: After hiding

After hiding the bit-s of the value-s in the pixel of cover image into 3x8 arrays only two least significant bits need to be changed or altered.

If there is a situation, where no match is found then the index bits will be changed to value 0.

During the decoding process, the index section is checked to determine the correct data. For this, 12 binary codes from 0000-1011 are used for decoding the data, while the code 1100 is used as a stop-bit. The remaining 3 unused codes, i.e. 1101, 1110, 1111 are used for a minimal level of error detection. Whenever the decoder detects any one of these 3 codes, it signals this as an error in transmission and reports the data to be corrupted.

III.OBSERVATIONS

Our proposed method is applied over different kinds of data and calculates the values of MSE and PSNR are resulted at a satisfactory level.

As the cover image has to be sufficiently large, we have used the nasa.bmp as the cover image all the times and we verify our method for various types of input data but here we will give only some of them, found after applying the proposed methods on the secret image or data. As secret text, we have taken some PPTs, PDFs and DOCs, since both of which are very essential in e-learning. In case of secret texts, we don’t apply the compressed algorithm, but in case of images, we apply both the compression algorithms. The table1 contains the

details of cover image; secret images are given in table2 and secret documents are given along with their MSE and PSNR values in table 3 and table 4, which we have used as the output of the observations.

Cover image		Nasa.bmp (3444x2484) 24.4MB
--------------------	--	-----------------------------------

Table1: Cover image along with their dimensions
Secret image




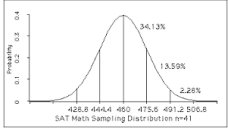






SI No.	Image	Name & Description
1.		Admit.png (667x645) 15.4 KB
2.		Marksheet.bmp (534x592) 9.14 KB
3.		108 Lord shiva temples.bmp (312x162) 148KB
4.		Math.png (297x170) 4.47KB
5.		peppers.bmp (512x512) 768KB
6.		Tagore statue.bmp (339x149) 148KB
7.		Image.png (191x264) 6.82KB
8.		E-Admit.png (689x857) 64.8KB
9.		Toad.bmp (220x188) 121KB
10.		Lab.bmp (340x148) 147KB

Table2: Set of secret images along with their dimensions

The following table shows the values of MSE and PSNR after applying the proposed method in the above secret images and some texts whose names details are given below. The outputs are shown after rounding off up to 4 decimal places.

Secret Image	MSE	PSNR
Admit.png	0.3769	52.4024
Marksheet.bmp	0.3019	53.3669
108 Lord shiva temples.bmp	0.2517	54.1557
Math.png	0.0073	69.5411
peppers.bmp	1.2702	47.1262
Tagore statue.bmp	0.2523	54.1454
Image.png	0.0113	67.6462
E-Admit.png	0.1063	57.8981
Toad.bmp	0.2043	55.0634
Lab.bmp	0.2530	54.1331

Table3: Table of outputs of secret images

Secret Text Files		
e-learning.pptx (uncompressed) (779KB)	1.2866	47.0703
Paper.pdf(uncompressed) (342KB)	0.1480	56.4622
Report.doc(compressed)(226 KB)	0.3759	52.4133
Score.pdf (104KB)	0.1762	57.7054
Paper1.doc(90.5KB)	0.1468	56.4981
Paper2.doc(132KB)	0.2166	54.8086
Paper3.docx(41.7KB)	0.0682	59.8276
Paper4.doc(792KB)	1.3087	46.9963
Example1.pdf(436KB)	0.7357	49.4978
Exempl2.pdf(354KB)	0.6034	50.3588

Table4: Table of outputs of secret Texts

If we carefully observe the above result, we can see that the proposed model is good for the documents which are lesser in size, since we can't apply the

compression algorithms on this kind of documents. But, in case of images, we have taken an image which is watermarked and the result is okay. Since, the size of mark sheet or admit card or the other e-learning testimonial documents are not very large in size, so our proposed model will provide good result for these.

IV. CONCLUSION

In this paper the proposed LSB-indexed method is applied for transacting e-learning testimonials on BMP and PNG image files in compressed form between administrator to learner, but it can also be applied in other kinds of images like TIFF or GIF except JPG or JPEG between the other participants of any e-learning system. It can also be applied in case of DOC and TXT file format. Other than e-learning, this model can be used in any cases where documents has to be sent secretly in any kind of online transaction system, like in e-commerce, e-governance etc. In case of compression algorithm, we can also apply any lossless compression algorithm, which will also be applicable for the documents other than image but it is out of scope of this paper.

REFERENCES

[1] Weippl, R.E., "Security in E-Learning", Springer, 2005
 [2] Talukdar, Kamrul Hasan and Koichi Harada, "Haar wavelet based approach for image compression and quality assessment of compressed image", arXiv preprint arXiv: 1010.4084(2010)
 [3] Adobe Developers Association, "TIFF (TM) Revision 6.0-Final", (1992)
 [4] Nag Akash and Karforma Sunil, "DSA security enhancement through efficient nonce generation", International Journal of Global Research in Computer Science, vol.5(10), pp:14-19, 2014
 [5] <https://en.wikipedia.org/wiki/Steganography>
 [6] <http://www.slideshare.net/SreelekshmiSree1/image-steganography-using-lsb>
 [7] T. Halder and S.Karforma, "A lsb-indexed steganographic approach to secure e-governance data", Second International Conference on Computing and Systems-2013, Department of computer science, The University of Burdwan, September 21-22, 2013, pp:158-163

Annexure

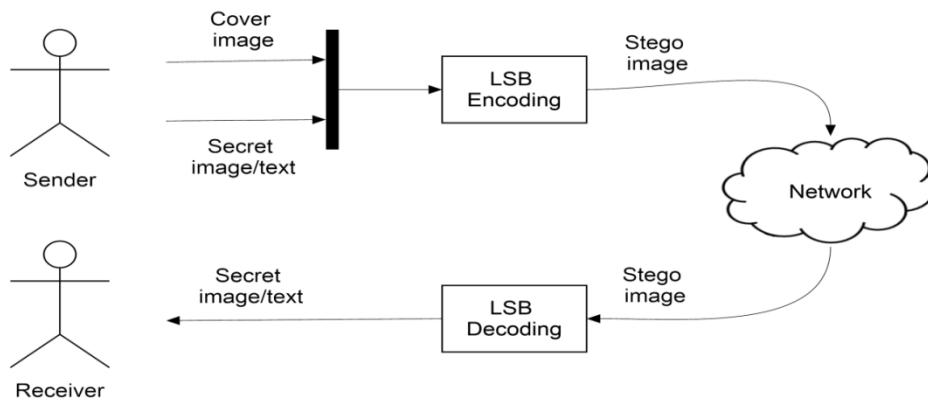


Fig.1: Diagram of transmission process without compression

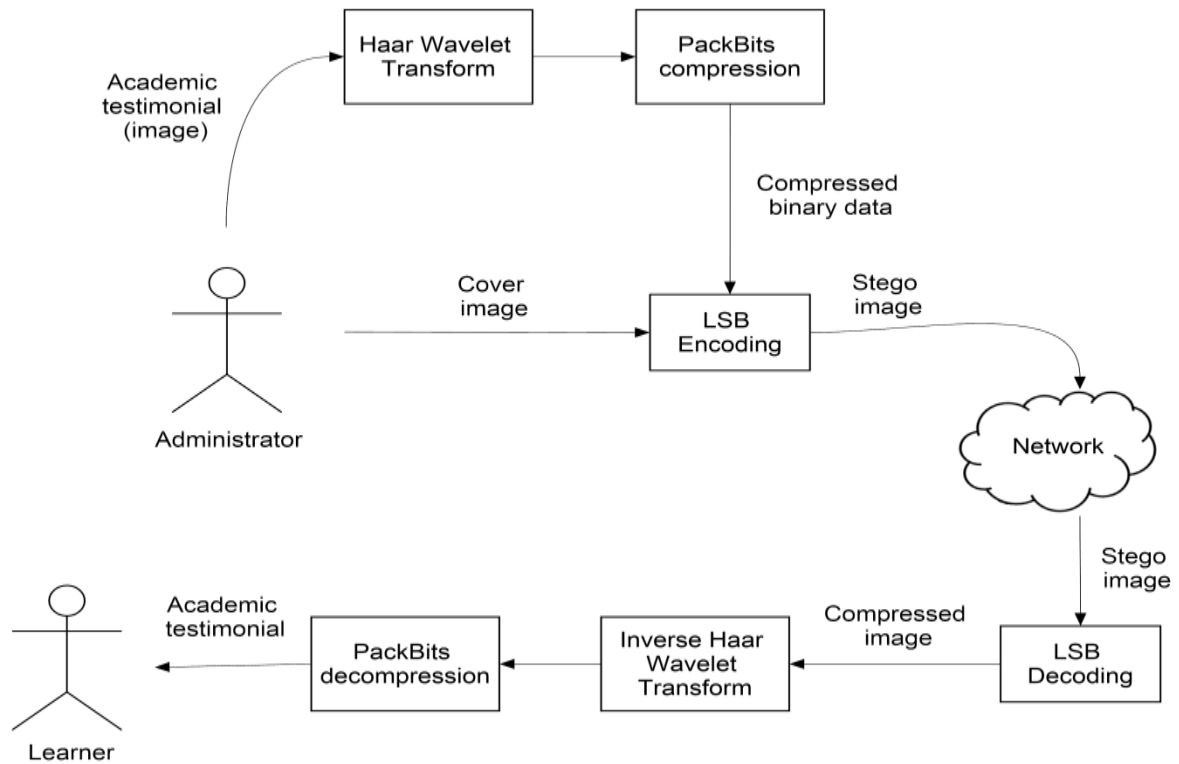


Fig.2: Diagram of transmission process with compression

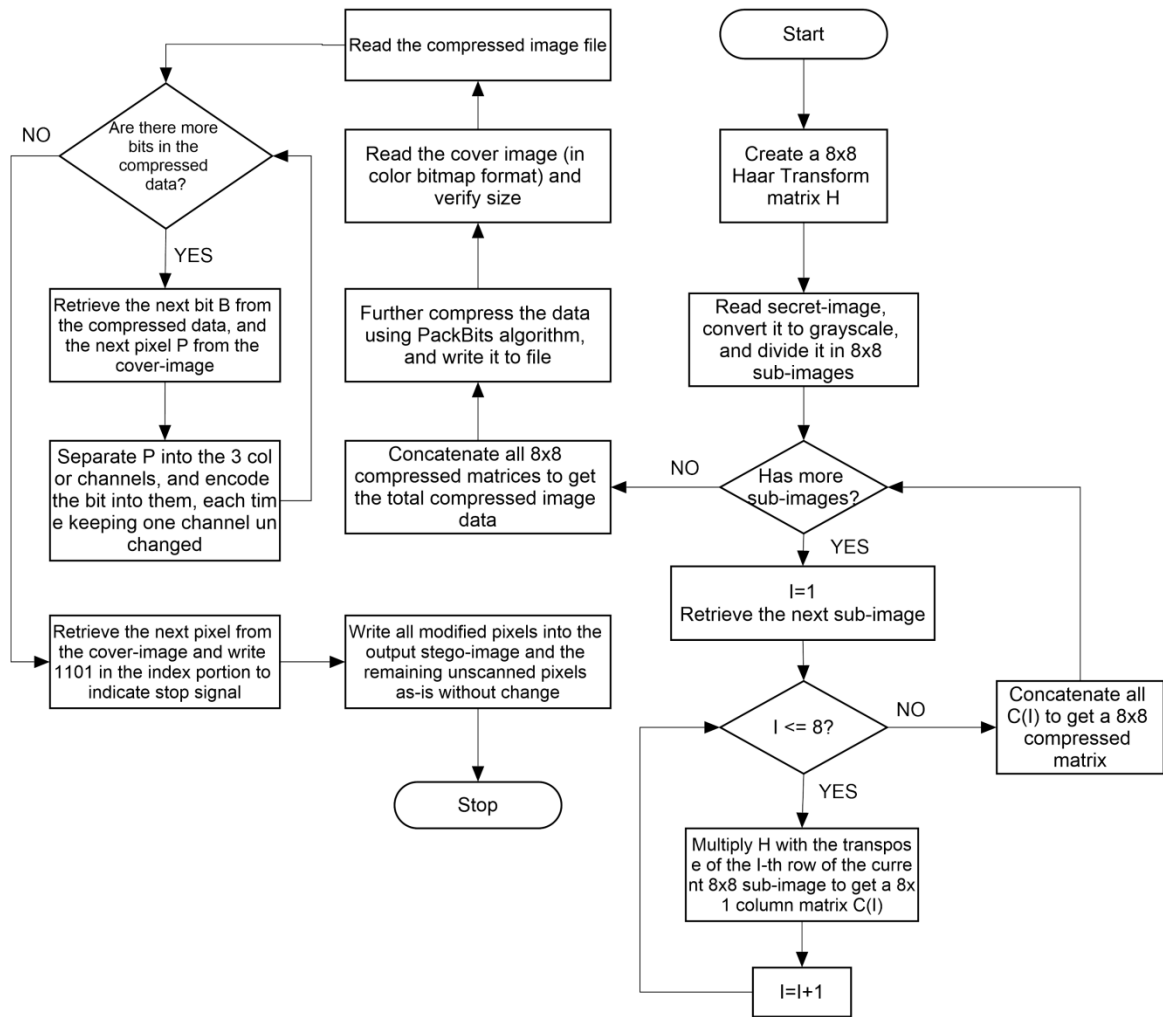


Fig.3: Flowchart of the proposed algorithm