STEGO-HUNTER :ATTACKING LSB BASED IMAGE STEGANOGRAPHIC TECHNIQUE

ABSTRACT :

Steganography is the process of hiding secret information in a cover image. Our aim is to test a set of images for statistical artifacts due to message embedding in color images using LSB insertion method and to find out, which images out of them are likely to be stego. In a natural uncompressed image (i.e. 24bit BMP) each image is represented by three color channels (Red, Green and Blue), each of the channel is 8 bits wide. The ratio of number of unique colors to the total number of pixels in an image is approximately 1:6 .If any test image is already tampered with message, embedding it further with additional bit streams will not modify the R value significantly. Alternately, if the test image is untampered one, the ratio R decreases significantly when it is further tampered by additional bit streams. Our decision of deciding the image as stego or untampered using the threshold value. After LSB embedding in natural image ,which is equivalent of introducing noise, the randomness of LSB pattern will increase. This will increase the number of close color pairs. We have chosen a deciding factor, that determines the given image as stego image or untampered image. If Deciding factor is greater than 100,then the image you have is an untampered image. Otherwise If Deciding factor is less than 100,then the image you have is an tampered image. We have done this experiment for about 60 images and the results are attached in this paper.

INTRODUCTION:

Steganography is the process of hiding secret information in a cover image. This process allows user to hide large amount of information with an image are in audio files. In this process, first we have to encrypt the secret data and then hide it in an innocent data. The stego medium is obtained by the addition of cover medium , hidden data and stego key. The cover medium is the file in which we hide our secret data (hidden data).The cover medium is typically an image file or audio files. The stego medium is also the same type of file in the cover medium. The stego image should not contain any easily detectable information by the human eye. The Steganographic tools are used to detect the hidden message in the stego medium.

STEGANOGRAPHIC METHODS:

There are several methods for hide our secret message in any image files or audio files. The commonly using approaches are as follows:

- Least Significant Bit (LSB) Insertion method.
- Frequency Domain Techniques.
- Spread Spectrum Techniques.
- Cover Generation methods
- Statistical methods.
- Fractal Techniques.

The stego image will vary according to the hidden messages. In pratical, the most widely using and simplest Steganographic method is LSB insertion method.

STEGANOGRAPHIC TOOLS:

The Steganographic tools are used to detect the secret data in the stego medium. The commonly used tools are as follows:

1.StegoDos.
2.MandelSteg.
3.Hide and Seek.
4.Jpeg-Jsteg.
5. S-Tools.
6. Ezstego.
7. Hide4PGP.
8. Steganos.

STEGO-ATTACK:

In this paper, we innovated a unique stego-only attack in LSB insertion for color images. This attack is applied when the stego-image is available and the attacker has no idea about the original cover image,stego key and encoding algorithm.It is almost the best feasible attack in real world.Our goal is to inspect a set of images for statistical artifacts due to message embedding in color images using LSB insertion method and to find out, which images out of them are likely to be stego.Our decision of deciding the image as stego or untampered using the threshold value. The selection of threshold value determines the robustness of our paper in terms of false detection in positive and negative sides. There is tremendous improvement in the performance which will be shown at last.

CLOSE COLOR PAIR ANALYSIS:

We have used a Steg-analysis method for uncompressed high-density color image format using the close color pair signature. In a natural uncompressed image (i.e. 24bit BMP) each image is represented by three color channels (Red, Green and Blue), each of the channel is 8 bits wide. Most methods hide the information in an uncompressed natural image which is based on replacing the LSB color channels by message bits. Thus, on the average only half of the LSB's are changed but ,the embedding message will not hamper the statistics of the cover image and in turn no detectable signatures will be generated.

In a natural uncompressed image, the ratio of number of unique colors to the total number of pixels is approximately 1:6.Hence after LSB embedding, which is equivalent of introducing noise, the randomness of LSB pattern will increase. This increase will reflected in increase in the number of close color pairs. We are considering two colors namely (R1,G1,B1) and (R2,G2,B2), If these two colors are close if and only if

$$|R1-R2|=1 \text{ and } |G1-G2|=1 \text{ and } |B1-B2|=1.$$

If these two colors are unique if and only if

$$|R1-R2|=1 \quad or \quad |G1-G2|=1 \quad or \quad |B1-B2|=1.$$

Next, we have to find the value of R which is the relative number of close color pairs with the unique colors where ,

$$R = P / U$$

We have observed that for an umtampered image (the image which does not contain any hidden message),the value of R is greater in comparison with the which has secret message embedded in it. This happens because the embedded message acts as a random noise ,which increases the number of unique colors abruptly.

As an example, we have taken five 24bit BMP images of different in color composition of birds,fruits,animals,building etc.The ratio of R for images is shown in below table. We done this experiment for 10% hiding alone. The result of R is tabulated in Tabulation 1.

At an absolute threshold ,the tampered water body image as untampered (false detection) one and an untampered land image as tampered (false alarm) one. After completed our testing, we have observed a particular property to distinguish the tampered image and an untampered image. The peculiar property is , if any test image is already tampered with a

Image Name	**Stego Image**	**Value of R**	**Value of R'**	**Value of m**

message, embedding it further with additional bit streams will not modify the R value significantly. Alternately, if the test image is untampered one, the ratio R decreases significantly when it is further tampered by additional bit streams.

If U' and P' are the number of unique colors and close color pairs respectively then,

$$R' = P' / U'$$

gives the relative number of close color pair in the artificially tampered image I'.

The change in the ratio R is measured in terms of m where, m is the percentage change in R defined as:

Ut_02ANI_cat.bmp	stego_02ANI_cat.bmp	37581	37566	0.0408
stego_02ANI_cat.bmp	stego_stego_02ANI_cat.bmp	37566	37567	-0.0027
Ut_02BIR_parrot.bmp	stego_02BIR_parrot.bmp	140280	139260	0.7257
stego_02BIR_parrot.bmp	stego_stego_02BIR_parrot.bmp	139260	139380	-0.0861
Ut_02BUI_taj.bmp	stego_02BUI_taj.bmp	121910	120270	1.3492
stego_02BUI_taj.bmp	stego_stego_02BUI_taj.bmp	120270	120320	-0.0474
Ut_04FLO_Tree-Peony	stego_04FLO_Tree-Peony	223630	223580	0.0261
stego_04FLO_Tree-Peony	stego_stego_04FLO_Tree-Peony	223580	223560	0.0048
Ut_06FRU_cocobannans.bmp	stego_06FRU_cocobannans.bmp	230270	228820	0.6303
stego_06FRU_cocobannans.bmp	stego_stego_06FRU_cocobannans.bmp	228820	228900	-0.0348

$$m = \frac{R - R'}{R'} * 100\ \%$$

Image Name	Stego Image	Value of P	Value of p’	Value of D	Proof
Ut_02ANI_cat.bmp	stego_02ANI_cat.bmp	9620757	9616834	100.0407931	Non Stego
stego_02ANI_cat.bmp	stego_stego_02ANI_cat.bmp	9616834	9617090	99.99733807	Stego
Ut_02BIR_parrot.bmp	stego_02BIR_parrot.bmp	35912028	35651431	100.730958	Non Stego
stego_02BIR_parrot.bmp	stego_stego_02BIR_parrot.bmp	35651431	35682142	99.91393174	Stego
Ut_02BUI_taj.bmp	stego_02BUI_taj.bmp	28039825	27661498	101.3677025	Non Stego
stego_02BUI_taj.bmp	stego_stego_02BUI_taj.bmp	27661498	27674623	99.95257388	Stego
Ut_04FLO_Tree-Peony	stego_04FLO_Tree-Peony	57250357	57235388	100.5893974	Non Stego
stego_04FLO_Tree-Peony	stego_stego_04FLO_Tree-Peony	57235388	57232618	99.99382229	Stego
Ut_06FRU_cocobannans.bmp	stego_06FRU_cocobannans.bmp	58948585	58577038	100.6342878	Non Stego
stego_06FRU_cocobannans.bmp	stego_stego_06FRU_cocobannans.bmp	58577038	58597420	99.9652169	Stego

TABULATION 1:

EVALUATION:

To distinguish the tampered image from an untampered image, the test we have done is,if deciding factor D

$$D = (P / P') * 100 \%$$

Where P is number of close color pair of an original image and P' is number of close color pair of stego image.

If D is greater than 100,then the image you have is an untampered image.Otherwise If D is less than 100,then the image you have is an tampered image.

We done an experiment taking approximately 50 BMP uncompressed images in various color combinations and performance results are shown in below table. There is an excellent improvement in the results shown below in Tabulation 2.

Conclusion:

The experimental results suggest that it is possible to reliably detect the presence of secret message embedded in uncompressed color images using LSB insertion technique. The reliability of detection depends on selection of threshold, which is an open ended problem. For some images it will break the condition. The variable threshold based on image statistics improves the correct detection rate.The results are attached in this paper.

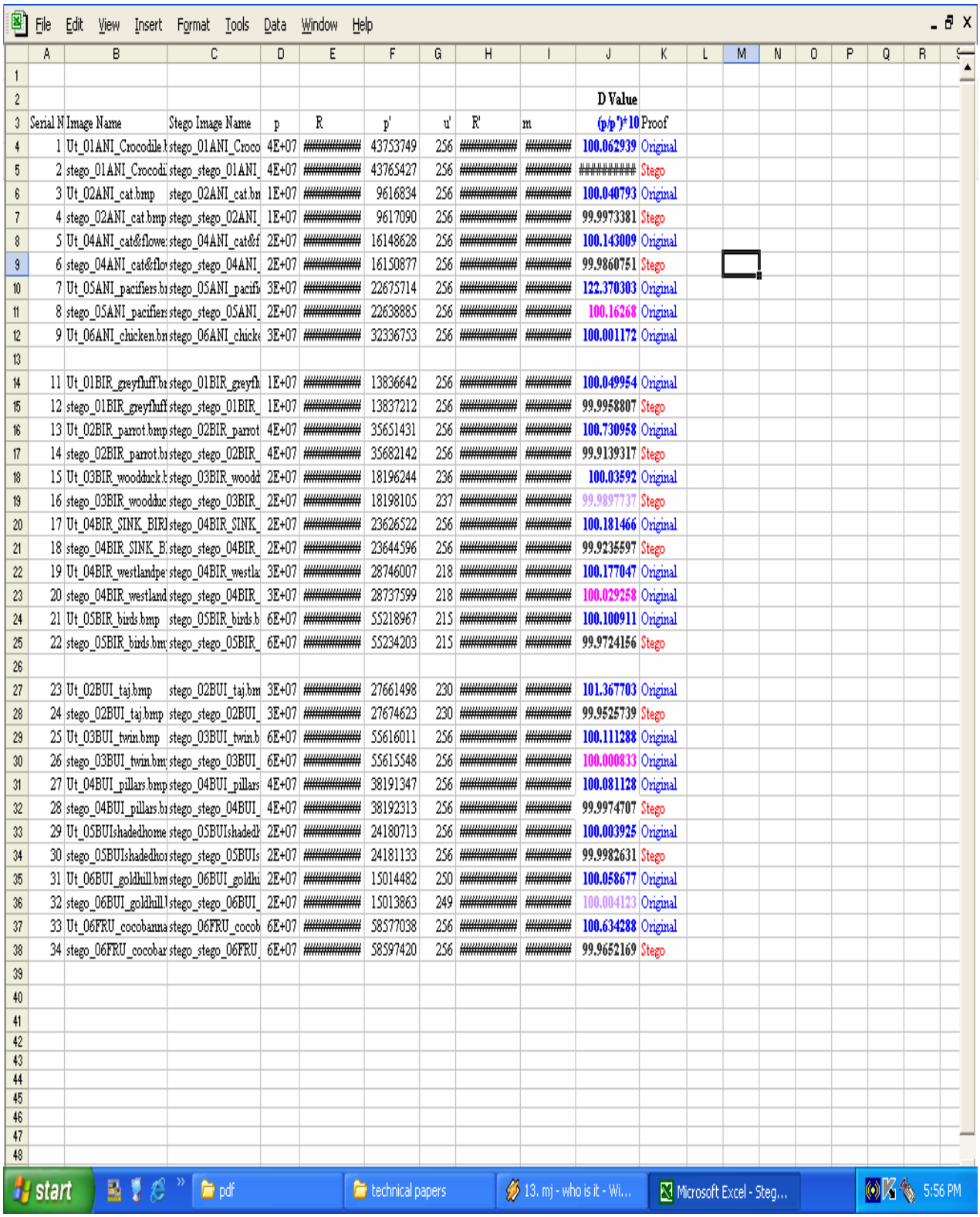
Sample Tested Images are shown below:

With this paper, the results for 40 images also attached .

Reference:

_www.Technicalpapers.co.nr

proof:



File Edit View Insert Format Tools Data Window Help

Serial N	Image Name	Stego Image Name	p	R	p'	u'	R'	m	D Value (p/p')*10	Proof
1	Ut_01ANI_Crocodile.b	stego_01ANI_Croco	4E+07	##########	43753749	256	##########	########	100.062939	Original
2	stego_01ANI_Crocodi	stego_stego_01ANI_	4E+07	##########	43765427	256	##########	########	##########	Stego
3	Ut_02ANI_cat.bmp	stego_02ANI_cat.bm	1E+07	##########	9616834	256	##########	########	100.040793	Original
4	stego_02ANI_cat.bmp	stego_stego_02ANI_	1E+07	##########	9617090	256	##########	########	99.9973381	Stego
5	Ut_04ANI_cat&flowe	stego_04ANI_cat&f	2E+07	##########	16148628	256	##########	########	100.143009	Original
6	stego_04ANI_cat&flo	stego_stego_04ANI_	2E+07	##########	16150877	256	##########	########	99.9860751	Stego
7	Ut_05ANI_pacifiers.b	stego_05ANI_pacifi	3E+07	##########	22675714	256	##########	########	122.370303	Original
8	stego_05ANI_pacifiers	stego_stego_05ANI_	2E+07	##########	22638885	256	##########	########	100.16268	Original
9	Ut_06ANI_chicken.bm	stego_06ANI_chicke	3E+07	##########	32336753	256	##########	########	100.001172	Original
11	Ut_01BIR_greyfluff.bi	stego_01BIR_greyfl	1E+07	##########	13836642	256	##########	########	100.049954	Original
12	stego_01BIR_greyfluff	stego_stego_01BIR_	1E+07	##########	13837212	256	##########	########	99.9958807	Stego
13	Ut_02BIR_parrot.bmp	stego_02BIR_parrot	4E+07	##########	35651431	256	##########	########	100.730958	Original
14	stego_02BIR_parrot.bi	stego_stego_02BIR_	4E+07	##########	35682142	256	##########	########	99.9139317	Stego
15	Ut_03BIR_woodduck.b	stego_03BIR_woodd	2E+07	##########	18196244	236	##########	########	100.03592	Original
16	stego_03BIR_woodduc	stego_stego_03BIR_	2E+07	##########	18198105	237	##########	########	99.9897737	Stego
17	Ut_04BIR_SINK_BIRI	stego_04BIR_SINK_	2E+07	##########	23626522	256	##########	########	100.181466	Original
18	stego_04BIR_SINK_B	stego_stego_04BIR_	2E+07	##########	23644596	256	##########	########	99.9235597	Stego
19	Ut_04BIR_westlandpe	stego_04BIR_westla	3E+07	##########	28746007	218	##########	########	100.177047	Original
20	stego_04BIR_westland	stego_stego_04BIR_	3E+07	##########	28737599	218	##########	########	100.029258	Original
21	Ut_05BIR_birds.bmp	stego_05BIR_birds.b	6E+07	##########	55218967	215	##########	########	100.100911	Original
22	stego_05BIR_birds.bm	stego_stego_05BIR_	6E+07	##########	55234203	215	##########	########	99.9724156	Stego
23	Ut_02BUI_taj.bmp	stego_02BUI_taj.bm	3E+07	##########	27661498	230	##########	########	101.367703	Original
24	stego_02BUI_taj.bmp	stego_stego_02BUI_	3E+07	##########	27674623	230	##########	########	99.9525739	Stego
25	Ut_03BUI_twin.bmp	stego_03BUI_twin.b	6E+07	##########	55616011	256	##########	########	100.111288	Original
26	stego_03BUI_twin.bm	stego_stego_03BUI_	6E+07	##########	55615548	256	##########	########	100.000833	Original
27	Ut_04BUI_pillars.bmp	stego_04BUI_pillars	4E+07	##########	38191347	256	##########	########	100.081128	Original
28	stego_04BUI_pillars.bi	stego_stego_04BUI_	4E+07	##########	38192313	256	##########	########	99.9974707	Stego
29	Ut_05BUIshadedhome	stego_05BUIshadedh	2E+07	##########	24180713	256	##########	########	100.003925	Original
30	stego_05BUIshadedhou	stego_stego_05BUIs	2E+07	##########	24181133	256	##########	########	99.9982631	Stego
31	Ut_06BUI_goldhill.bm	stego_06BUI_goldhi	2E+07	##########	15014482	250	##########	########	100.058677	Original
32	stego_06BUI_goldhill.l	stego_stego_06BUI_	2E+07	##########	15013863	249	##########	########	100.004123	Original
33	Ut_06FRU_cocobanna	stego_06FRU_cocob	6E+07	##########	58577038	256	##########	########	100.634288	Original
34	stego_06FRU_cocobar	stego_stego_06FRU_	6E+07	##########	58597420	256	##########	########	99.9652169	Stego

start | pdf | technical papers | 13. mj - who is it - Wi... | Microsoft Excel - Steg... | 5:56 PM