A Steganographic Performance Comparison of the C_4S Algorithm with selected SSIS Algorithms

Student Name: Qingyang Feng (980940)
Principal Supervisor: Prof. Udaya Parampalli
Co-Supervisor: Dr. Peter Eze

August 2023

Introduction

- **Steganography** is an Information Hiding (IH) technique to hide secret messages in cover data such as audio, videos and images.
- **Spread Spectrum** (SS) is a popular steganography technique due to its robustness against attacks. In a generalised SS Image Steganography (SSIS) system, the secret message is embedded with an additive embedding function:

$$Y_{ij} = X_{ij} + \alpha W_{ij} (-1)^{S_i}$$

where X is the original cover image, α is the embedding strength, W is a pseudorandom noise signal, S is the secret message and Y is the stego image.
To extract the message:

$$S_i' = \begin{cases} 0 & corr(Y_{ij}, W_{ij}) > 0 \\ 1 & corr(Y_{ij}, W_{ij}) < 0 \end{cases}$$

Introduction

- Limitation of generalised SS: low data carrying capacity.
- A new **Constant Correlation Compression Coding Scheme (C_4S)** [2] was developed to improve the capacity and the watermark detection accuracy of the generalised SS
- The purpose of this project is to study the performance of the C_4S algorithm in comparison with two other SSIS algorithms, that of Kumar et al. [3] and Naseem et al. [4], in terms of
  - distortion
  - steganographic capacity
  - effect on machine-based diagnostic systems
  - ability for tamper detection
  - robustness to attack

Constant Correlation Compression Coding Scheme (C_4S)

- Host Signal Interference (HSI): the correlation is not always zero for a sub-block without watermarking which leads to false positives for watermark detection.
- **Constant Correlation** to eliminate HSI and ensure accurate watermark detection: dynamically computes the embedding strength α with a chosen constant correlation value p

$$\alpha_{0,1} = \frac{pmn - \sum_{i=1}^{m} \sum_{j=1}^{n} X_{ij} W_{ij} (-1)^{S_i}}{\sum_{i=1}^{m} \sum_{j=1}^{n} W_{ij}^2}$$

- **Compression Encoding** to increase embedding capacity: a group of cr binary bits rather than a single bit is embedded into each sub-block by choosing 2^{cr} different constant correlation values instead of one p value.

Kumar SS

- To embed data:
  - Discrete Wavelet Transform (DWT) is performed on the cover image
  - The watermark bits are embedded in the vertical (ccV) and horizontal (ccH) second level subband coefficients with different PN sequence pairs (PN_h and PN_v): For each watermark bit, if the bit $= 0$,

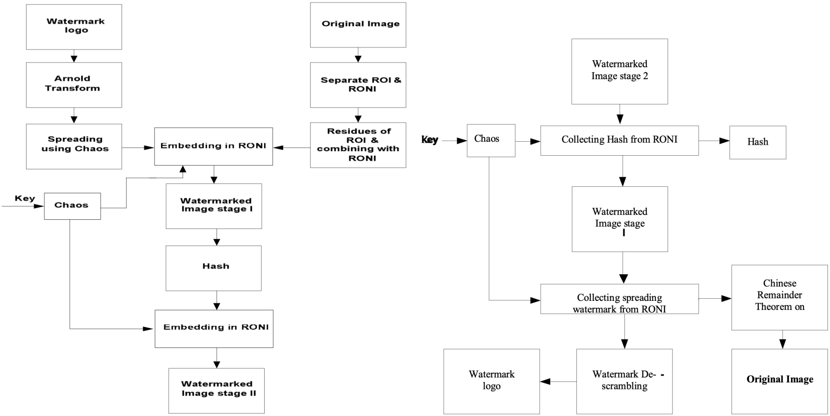
    $$ccH = ccH + k * PN_h$$
    $$ccV = ccV + k * PN_v$$

    where k is the embedding strength.
  - Retrieve by applying the inverse DWT with updated subband coefficients
- To extract data:

$$corr_H = \text{correlation between } PN_h \text{ and } ccH$$
$$corr_V = \text{correlation between } PN_v \text{ and } ccV$$
$$avg_{corr} = (corr_H + corr_V)/2$$

If avg_{corr} is above the average value over all watermark bits, the corresponding watermark bit is "0", otherwise it is "1".

Naseem SS

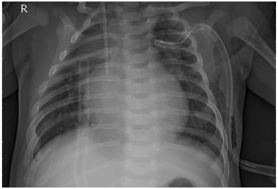


(a) Data Embedding (b) Data Extraction

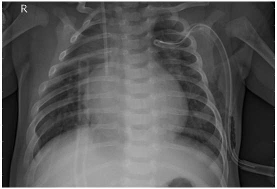
Figure: Nassem SS

Stego Images

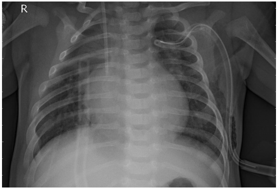
The algorithms are experimented on Chest X-ray images:



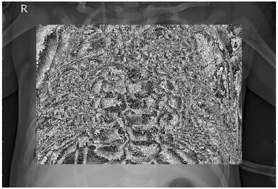
(a) Original Image



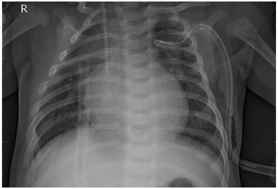
(b) C_4S



(c) KumarSS



(d) NaseemSS with residued ROI



(e) NaseemSS with recovered ROI

Figure: Images watermarked by different algorithms.

Parameter Tuning

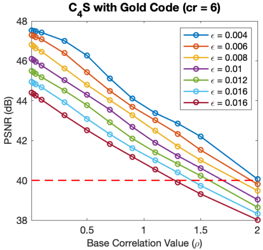
The parameters of each algorithm are tuned based on three measurements:

- **Peak Signal-to-Noise Ratio (PSNR)**: measures the statistical imperceptibility of the watermark. The greater PSNR is the less imperceptible the degradation is. An effective IH algorithm commonly requires a PSNR of 40dB or greater.
- **Structural Similarity Index (SSIM)**: measures the visual imperceptibility of the watermark. The greater SSIM is, the more similar the two images are.
- **Bit Error Rate (BER)**: measures the accuracy of the extraction of the watermark. It is computed by the ratio of the number of bits that are wrongly extracted by the total number of embedde bits

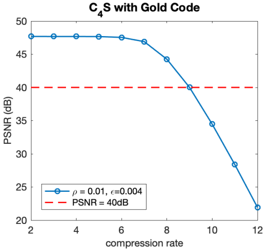
The optimal combination of parameters is selected for each algorithm by grid search.

Parameter Tuning

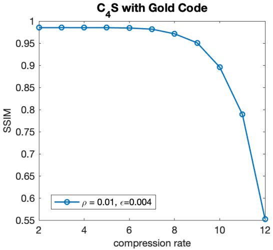
- C_4S: $\rho = 0.01$, $\epsilon = 0.004$, compression rate $= 8$



(a) Average PSNR with different values of BCV (ρ) and fault tolarence (ϵ).



(b) Average PSNR with $\rho = 0.01$, $\epsilon = 0.004$ and different cr.



(c) Average SSIM with $\rho = 0.01$, $\epsilon = 0.004$ and different cr.

Figure: Parameter Tuning for C_4S

Parameter Tuning

- Kumar: embedding strength $= 0.2$, embedding rate $= 0.0002bpp$.

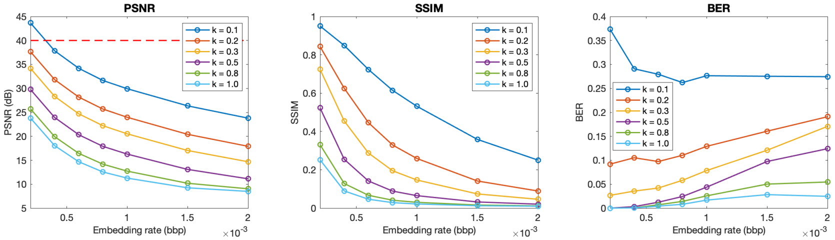


Figure: Average PSNR/SSIM/BER with different embedding rate and embedding strength (k).

- *Naseem*: chip rate $= 2$

Chip Rate (cr)	1	2	4	8	16	32	64
Embedding Rate (bpp)	0.0761	0.0380	0.0190	0.0095	0.0048	0.0024	0.0012
PSNR (dB)	43.7737	43.7748	43.7769	43.7790	43.7730	43.7736	43.7718
SSIM	0.996	0.996	0.996	0.995	0.996	0.995	0.996
BER	0.48998	0.07722	0.07309	0.06352	0.04838	0.01949	0.00279

Table: Embedding rate and average PSNR/SSIM/BER with different chip rates.

Measurements after Parameter Tuning

Algorithm	Embedding Rate (bpp)	PSNR (dB)	SSIM	BER (%)
KumarSS [3]	0.0002	37.4867	0.9281	7.4560
NaseemSS [4]	0.0380	44.0699	0.9922	6.6982
C_4S [2]	0.1250	43.6326	0.9614	0

Table: Embedding rate and average PSNR/SSIM/BER by different algorithms.

- C_4S produces the highest embedding rate at a high PSNR ($43.6326dB$) and SSIM (0.9614).
- C_4S is the only algorithm among the three that achieved zero BER which makes it suitable for embedding text-based watermarks.
- NaseemSS outperforms C_4S in imperceptibility but the two are very close.

Evaluation Framework

The three algorithms are evaluated with the framework proposed by Eze et al. [1]. The evaluation criteria included in the framework are:

- **Integrity score** I_{sc}: measures the percentage of sub-blocks with attacks being correctly detected by the *ItegrityChecker*.
- **Privacy Score** P_{sc}: measures privacy by the accuracy of watermark extraction and the ability to hide the information in cover without easy detection by an unauthorised party.
- **Distortion Score** DT_{sc}: measures the relative distortion introduce by hidden information of a certain algorithm among all considering algorithms.

Evaluation Framework

- **SVM Accuracy**: measures the classification accuracy of a Support Vector Machine (SVM) trained on biomarkers extracted from the images watermarked by each of the three algorithms. The biomarkers considered in this work are contrast, energy, homogeneity and entropy extracted from the Region of Interest (ROI) of the chest X-rays.
- **Location Change Score** LC_{sc}: measures the percentage deviation in value of a biomarker caused by data embedding.
- **Dispersion Score** D_{sc}: measures the tendency of the algorithm to alter disease classification by machine based systems or humans.
- **Attack Response**: measures the ability to extract the hidden information after attack. The four attacks considered in this project are Gaussian Noise, Speckle Noise, Salt and Pepper Noise and Contrast Adjustment.
- **Average Score**: the average score of the considered criteria

Evaluation Score

Criteria	*KumarSS*	*NaseemSS*	C_4S
Integrity Score (I_{sc})	0	1	77.72
Privacy Score (P_{sc})	46.35	61.85	100
Distortion Score (DT_{sc})	0 (37.49)	35.20	34.85
Location Change Score (LC_{sc})	49.79	100	81.54
Dispersion Score (D_{sc})	87.79	100	99.52
SVM Accuracy	93.67	99.00	66.33
Attack Response	75.82	78.99	44.91
Average Score	50.49	68.01	72.12

Table: Values of Evaluation Criteria for the three selected SSIS

Conclusion

Compared to the two other algorithms, the advantages of C_4S are

- C_4S has a much higher embedding capacity with an effective PSNR of 43.63dB: three times more than *NaseemSS* and 600 times more than *KumarSS*.
- When the watermarked image is not tampered with, zero BER can be achieved by C_4S for all compression rates between 2 and 12.
- Localised tamper detection is available with high detection rate (77.72%) while there is no tamper detection for Kumar and only global tamper detection for Naseem.

The disadvantages of C_4S are

- It is found to be less robust against contrast adjustment attacks and noise addition attacks.
- It is also found to have a more significant negative effect on SVM classification accuracy.
- Both may be caused by the high compression rate (8) chosen for the implementation.

Future Work

- To choose a lower compression rate on C_4S and evaluate its effect on the evaluation criteria
- To choose a different spreading sequence for C_4S and compare it with the gold code used in the project
- To evaluate the algorithms on other types of medical images such as ultrasound, CT scans and MRI scans.
- To implement other algorithms and include them in the comparison.

References

[1] Peter Eze, Udaya Parampalli, Robin Evans, and Dongxi Liu. A new evaluation method for medical image information hiding techniques. In *2020 42nd annual international conference of the IEEE engineering in Medicine & Biology Society (EMBC)*, pages 6119–6122. IEEE, 2020.

[2] Peter U Eze, Udaya Parampalli, Robin J Evans, and Dongxi Liu. Spread spectrum steganographic capacity improvement for medical image security in teleradiology. In *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 1–4. IEEE, 2018.

[3] Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan, et al. Secure spread-spectrum watermarking for telemedicine applications. *Journal of Information Security*, 2(02):91, 2011.

[4] Muhammad Tahir Naseem, Ijaz Mansoor Qureshi, Muhammad Zeeshan Muzaffar, and Atta ur Rahman 0001. Spread spectrum based invertible watermarking for medical images using rns and chaos. *Int. Arab J. Inf. Technol.*, 13(2):223–231, 2016.