engineering proceedings

MDPI

Proceeding Paper

Personal Social Network Profile Authentication through Image Steganography †

Subhadip Mukherjee [1], Somnath Mukhopadhyay [2] and Sunita Sarkar [1,*]

[1] Department of Computer Science and Engineering, Assam University, Silchar 788011, Assam, India; itissubhadip@gmail.com
[2] Department of Computer Application, Sikkim University, Gangtok 737102, Sikkim, India; som.cse@live.com
* Correspondence: sarkarsunita2601@gmail.com
† Presented at the 4th International Electronic Conference on Applied Sciences, 27 October–10 November 2023; Available online: https://asec2023.sciforum.net/.

Abstract: In the era of digital communication and social networking, the authenticity and integrity of personal social network profiles have become crucial for establishing trust and ensuring secure interactions. Existing methods often suffer from vulnerabilities like password theft, identity impersonation, and data breaches. To overcome these challenges, the paper introduces a new steganography method as a robust solution, leveraging the concept of hiding information within a seemingly innocent digital cover image. The proposed methodology involves imperceptible authentication and embedding profile information within a profile image or any other uploaded pictures in a profile's timeline. This scheme is developed using a shell matrix, DNA encoding and absolute moment block truncation coding (AMBTC) compression. A shell matrix is used for concealing the private information and AMBTC compression is applied to compress large data files into smaller ones, which can speed up the network transmission of compressed code. By exploiting the redundancy in image data, the authentication data are embedded in a manner that is indistinguishable to human observers. To estimate the effectiveness of the proposed approach, wide experiments were conducted using real-world social network profiles. The results demonstrate the ability of the proposed technique to successfully embed and extract authentication data while maintaining the profile photo's visual appearance.

Keywords: shell matrix; covert communication; AMBTC compression; multimedia security; social media security

Citation: Mukherjee, S.; Mukhopadhyay, S.; Sarkar, S. Personal Social Network Profile Authentication through Image Steganography. *Eng. Proc.* **2023**, *56*, 129. https://doi.org/10.3390/ASEC2023-16635

Academic Editor: Alessandro Bruno

Published: 15 December 2023

1. Introduction

Securing a social media profile includes the practice of examining live multimedia data to protect against threats and security breaches. The risks specific to each sector vary, and the same applies to social media. These perils may include preventing intended phishing attacks, protecting business profiles from unauthorised access, fighting fraud, or avoiding social engineering scams like profile mimicry. Security of multimedia data over social media is essential for modern business or personal success. We can post certain publicly accessible material on all social media networks. Without your consent, others might treat you as a public entity. Depending on the privacy settings, approved contacts may copy and repost content, including images or personal information, without the user's permission. The security of the information that has been published on a profile may not always be guaranteed by social networks, even when posts are ostensibly private.

Steganography is a method for maintaining the security of multimedia data by concealing sensitive information in a cover file [1–3]. In 2014, the first image steganography technique depending on a turtle-shell matrix structure was suggested with 1.5 bpp of EC [4]. In 2015, ref. [5] introduced an octagon-shell matrix-oriented information hiding system with 2.0 bpp of EC. In 2017, a hiding technique was suggested where in order to

conceal a secret number in an X-ary notational system, the values of the pair of pixels in the original image are altered in accordance with instructions provided by the turtle shell [6]. With reversibility and higher payload, another shell matrix-based work for concealing information in dual pictures was suggested in 2021 [7]. In 2022, Mukherjee et al. suggested a novel steganography method depending on a multi-layered shell matrix that can insert six bits within each pair of pixels results in 3.0 bpp of hiding capability and an average PSNR value of 48.40 dB [8]. In [9], the suggested technique works by determining the reference set for each pair of pixels in the octagon matrix for inserting a private digit. The cover pixel pair can then be updated using the corresponding set with minor distortion. Being a less computationally intensive method, the human visual system can be avoided. In recent years, research on information security has been carried out on DNA-based data hiding schemes [10,11]. DNA sequencing is the process of determining the nucleic acid sequence or the arrangement of nucleotides in DNA. The sequence is composed of the four nucleotide bases: cytosine, adenine, thymine, and guanine. The biological information that cells use to advancement and function is arranged in the base arrangement. In today's fast-paced digital world, social network website performance and user experience are key factors that can make or break a business. A slow-loading social network website can result in a high bounce rate, which means losing potential profiles. This is where image compression comes in: AMBTC image compression is the process of reducing the file size of an image without significantly impacting its quality [12,13]. By compressing images, the overall size of an image as well as social network website can be diminished, leading to quicker loading times and improved customer experience.

In this paper, we have proposed a multimedia security system with a compressed image steganography technique for securing social network profiles and covert communications over social network platforms like Facebook, Instagram, LinkedIn, etc. By using our proposed technique, we can hide profile details within a profile picture or any uploaded picture in social media for profile authentication. One can establish a covert communication through image chat in any social media platform. By adopting the proposed method, a social media company can achieve multimedia data security, e.g., Facebook, Instagram, LinkedIn, etc. can easily identify from which profile a particular picture was uploaded for the first time. This article is arranged into the following sections: In Section 2, the proposed embedding and extraction procedures are described. In Section 3, experimental outcomes are illustrated. The conclusion is specified in Section 4.

2. Proposed Work

In social networks, people generally use colour photos, which is the reason we have proposed our steganography technique for use in RGB colour images. In our steganographic approach, we first compress the image using the AMBTC strategy and then hide the secret information within the compressed cover image to obtain the stego compressed image (see Figure 1). We have applied a DNA encoding rule like C $\rightarrow$ 00, T $\rightarrow$ 11, G $\rightarrow$ 10, and A$\rightarrow$ 01 to obtain an equivalent bitstream or vice versa. For enhancing the security of our approach, we have selected a publicly available DNA sequence as reference DNA (R_d). Moreover, we obtain an encrypted DNA sequence by performing a XOR operation between R_d and the DNA-encoded secret information. One of the rules of the DNA sequence XOR operation is the following: A $\oplus$ A = A, G $\oplus$ C = T, G $\oplus$ G = A, C $\oplus$ A = C, T $\oplus$ G = C, G $\oplus$ A = G, A $\oplus$ T = T, C $\oplus$ C = A, C $\oplus$ T = G, T $\oplus$ T = A.

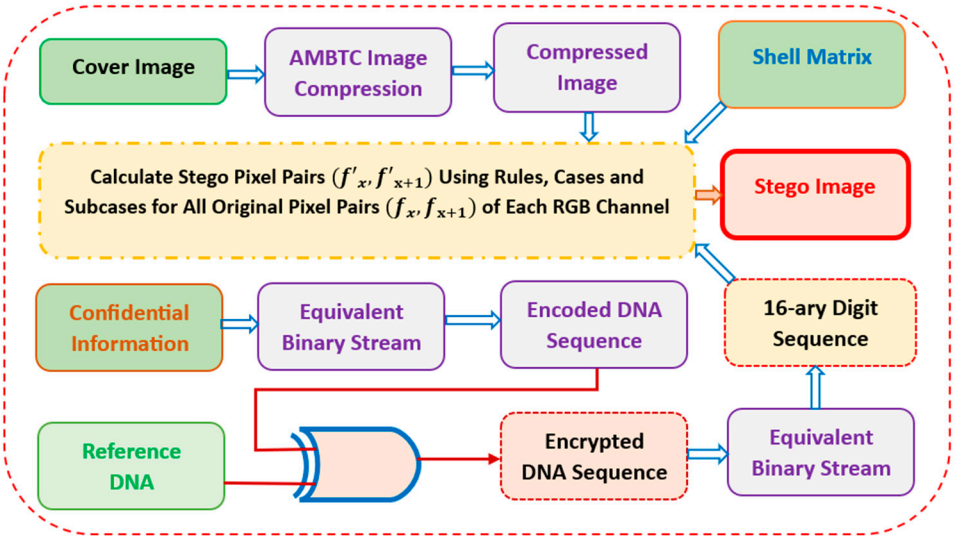

Figure 1. Block Diagram of Embedding.

2.1. Embedding Procedure

Step 1: Input a M × N colour image, a reference DNA (R_d), and the secret information.

Step 2: Generate the RGB channels of the image. Convert the secret information into a bitstream B_s.

Step 3: Select a channel and divide it into 4 × 4 blocks.

Step 4: For each block, calculate the mean via Equation (1):

$$R = \frac{1}{16} \sum_{y=1}^{4} \sum_{z=1}^{4} r(y,z) \tag{1}$$

Step 5: Divide the elements into two subgroups, i.e., sg_1 and sg_2, according to Equation (2):

$$r(y,z) = \begin{cases} sg_1 & if\ r(y,z) < R \\ sg_2 & if\ r(y,z) \geq R \end{cases} \tag{2}$$

Step 6: Calculate two quantisation procedures via Equations (3) and (4):

$$L = \frac{1}{n(sg_1)} \sum_{y=1}^{4} \sum_{z=1}^{4} r(y,z) \qquad where,\ r(y,z) \in sg_1 \tag{3}$$

$$H = \frac{1}{n(sg_2)} \sum_{y=1}^{4} \sum_{z=1}^{4} r(y,z) \qquad where, r(y,z) \in sg_2 \tag{4}$$

where $n(sg_1)$ and $n(sg_2)$ are the number of elements in sg_1 and sg_2, respectively.

Step 7: Now, replace all the elements of sg_1 by L and sg_2 by H. This will generate the compressed block.

Step 8: Select the next block and apply steps 4 to 7 to obtain the compressed block. Do this until all the blocks of the current channel are compressed.

Step 9: By following steps 3 to 8, compress all the channels and generate the compressed image.

Step 10: Generate the DNA sequence (S_d) of B_s using the DNA encoding rule. Perform the XOR operation among the nucleotides of S_d and R_d and generate the encrypted DNA sequence E_d. Generate the bitstream from E_d using the same encoding rule. Split this bitstream into groups of 4 bits. Construct a sequence of 16-ary digits from the 4 bit groups.

Step 11: Construct the octagon shell matrix S_m of size 256 × 256 by performing the following: (1) select a starting digit for the (0,0) coordinate within the range from 0 to 15; (2) based on the starting digit, generate all the values of S_m by a value difference of 1 for the same row as well as 4 and 5 for same column alternatively within the range from 0 to 15.

Step 12: Select an RGB channel and divide it into a non-overlapping pixel pairs (f_x, f_{x+1}) where $x \in \{1, 3, \ldots, M \times N - 1\}$.

Step 13: Select a secret digit d_s and a pixel pair (f_x, f_{x+1}) of the original colour channel where ds is to be hidden. Then hide d_s within (f_x, f_{x+1}) by using the following rules and obtaining the stego pixel pair (f'_x, f'_{x+1}):

Rule A: If the digit at (f_x, f_{x+1}) in S_m, i.e., $S_m(f_x, f_{x+1})$, equals to ds then (f_x, f_{x+1}) is itself the sego pixel pair of the original pair (f_x, f_{x+1}), i.e., $(f'_x, f'_{x+1}) = (f_x, f_{x+1})$.

Rule B: If $S_m(f_x, f_{x+1}) \neq d_s$, then find a pixel pair (f'_x, f'_{x+1}) as the stego pixel pair in S_m by using the following cases:

Case A: If $S_m(f_x, f_{x+1})$ is situated inside a shell, then find the closest pixel pair (f'_x, f'_{x+1}) from (f_x, f_{x+1}) within that shell where $S_m(f'_x, f'_{x+1}) = d_s$. Replace (f_x, f_{x+1}) by using the stego pixel pair (f'_x, f'_{x+1}).

Case B: If $S_m(f_x, f_{x+1})$ is not situated inside a shell, then use the following subcases:

Subcase A: If $S_m(f_x, f_{x+1})$ is situated on either the last or first column or first or last row the of S_m, then reference set R_s is calculated by using a 5×5 block which involves $S_m(f_x, f_{x+1})$ at the middle of that last or first column or first or last row of that square (see the yellow square in Figure 2). Now, find the shortest distance $S_m(f'_x, f'_{x+1})$ from $S_m(f_x, f_{x+1})$ in R_s where $S_m(f'_x, f'_{x+1}) = d_s$. Replace (f_x, f_{x+1}) by using the stego pixel pair (f'_x, f'_{x+1}).

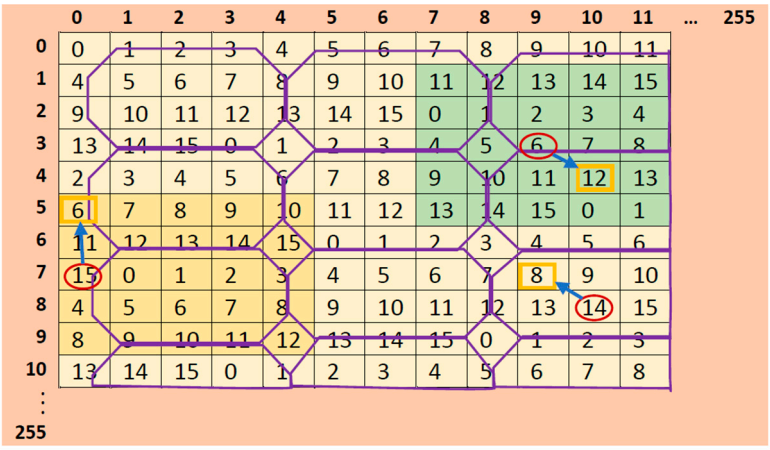

Figure 2. Example of the proposed shell matrix.

Subcase B: If $S_m(f_x, f_{x+1})$ does not come under subcase A, then reference set R_s is calculated by using a 5×5 block where $S_m(f_x, f_{x+1})$ is situated at the centre of the block (see the green square in Figure 2). Now, find the shortest distance $S_m(f'_x, f'_{x+1})$ from $S_m(f_x, f_{x+1})$ in R_s where $S_m(f'_x, f'_{x+1}) = ds$. Replace (f_x, f_{x+1}) by using the stego pixel pair (f'_x, f'_{x+1}).

Step 14: Hide all the secret digits by repeating step 13 and generate the stego colour channel.

Step 15: Follow step 12 to 14 to hide all the secret digits within all three RGB channels and generate the stego colour image.

2.2. Extraction Procedure

Obtain three RGB channels from the stego-compressed image and split each channel into non-overlapping pixel pairs (f'_x, f'_{x+1}) where $x \in \{1, 3, \ldots, M \times N - 1\}$. Construct the Sm by using the same construction rules used in the hiding method. For every channel, select each pixel pair (f'_x, f'_{x+1}) and, by mapping it to the S_m, find the hidden 16-ary secret digit. Repeat this mapping for all the pixel pairs of each channel and obtain the secret digit stream. Convert this 16-ary digit into bitstream. Convert this bitstream into the DNA sequence (K_d) using the same encoding rule which was used for data embedding. Apply the XOR operation between R_d and K_d using the same rule applied in the embedding phase

and obtain the new DNA sequence (N_d). Convert this N_d into bitstream using the same encoding rule. Obtain the original message from this bitstream.

Considering Figure 2, assume that we need to hide the secret digits 6, 12, and 8 within the pixel pairs (7, 0), (3, 9), and (8, 10), and then according to Subcase A, Subcase B, and Case A, the stego pixel pairs will be (5,0), (4,10), and (7,9).

3. Experimental Results

Test photos from the USC-SIPI were utilised for various experiments in this study [14]. The pictures with a 256 × 256 size were (a) a tree, (b) a baboon, (c) an airplane, (d) and peppers. In our experiments, reference DNA sequences were taken from [15–17]. The stego image quality evaluation parameter PSNR [18,19] is used to evaluate the proposed method performance with different embedding rates (ERs). In Table 1, the metrics payload in bits, the PSNR in dB, and the EC in bpp for different images are presented. We have obtained the maximum EC of 2.00 bpp. In Table 2, the highest ECs are compared with other recent and existing methods [10–12] (for TH = 30) and [13] (for d_{th} = 16) are displayed. It is clear that our approach has obtained a much higher capacity than [10–13] (see Figure 3).

Table 1. Outcomes of the proposed work.

Image	Payload (Bits)	PSNR (dB)	EC (bpp)
Tree	65,536 131,072	34.44 29.52	1.00 2.00
Baboon	65,536 131,072	34.94 29.67	1.00 2.00
Airplane	65,536 131,072	34.19 29.54	1.00 2.00
Peppers	65,536 131,072	34.65 29.81	1.00 2.00

Table 2. Comparisons with other works (in bpp).

Works	Tree	Baboon	Airplane	Peppers
Horng [13]	between 0.80 and 1.28	0.80	1.19	1.24
Firas [10]	0.69	0.69	0.69	0.69
Subhadip [11]	0.78	0.78	0.78	0.78
Chin [12]	between 0.88 and 1.22	0.88	1.17	1.22
Proposed	2.00	2.00	2.00	2.00

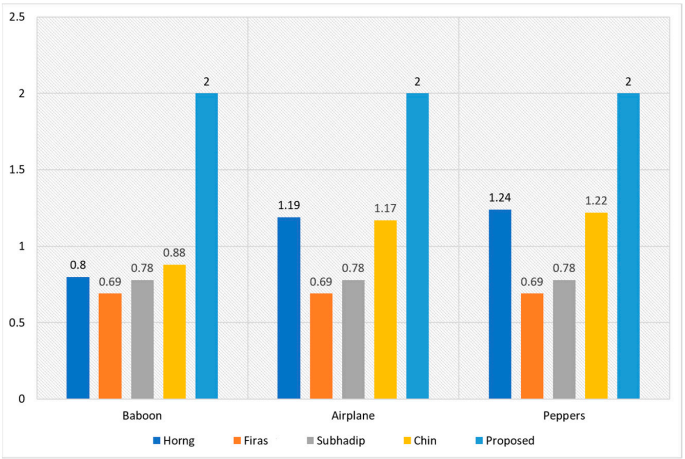

Figure 3. EC comparison (in bpp) with other methods [10–13].

Approximately 163 million DNA sequences are accessible to the general public. The probability of predicting reference DNA sequence is $\frac{1}{1.63\times10^8}$. The number of the binary coding rules is 4! = 24 and the number of XOR combinations is 2^{8m} where m is the size of the message. Therefore, the final cracking probability of the DNA encryption = $\frac{1}{2^{8m}} \times \frac{1}{24} \times \frac{1}{1.63\times10^8}$.

4. Conclusions

Social media is such an important part of how we communicate and engage with each other online, and we all need to approach it with more caution. It involves sharing information, exchanging feedback, creating content, etc. In this article, a multimedia security method was designed using image steganography. Here, the AMBTC image compression was applied for faster covert communication over social media. This image steganography approach has achieved 2.00 bpp of EC with $\frac{1}{2^{8m}} \times \frac{1}{24} \times \frac{1}{1.63\times10^8}$ DNA encryption cracking probability. By using our proposed technique, we can hide profile details within a profile picture or any uploaded picture for authentication. A social media company can easily identify from which profile a picture was uploaded for the first time. One can establish a covert communication through image chat in any social media platform.

Author Contributions: Conceptualisation, S.M. (Subhadip Mukherjee) and S.S.; methodology, S.M. (Subhadip Mukherjee); software, S.M. (Subhadip Mukherjee) and S.M. (Somnath Mukhopadhyay); validation, S.M. (Subhadip Mukherjee), S.S., and S.M. (Somnath Mukhopadhyay); formal analysis, S.M. (Subhadip Mukherjee); investigation, S.M. (Subhadip Mukherjee) and S.S.; resources, S.M. (Subhadip Mukherjee); data curation, S.M. (Subhadip Mukherjee); writing—original draft preparation, S.M. (Subhadip Mukherjee); writing—review and editing, S.S. and S.M. (Somnath Mukhopadhyay); visualisation, S.M. (Subhadip Mukherjee); supervision, S.S. and S.M. (Somnath Mukhopadhyay). All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mukherjee, S.; Sarkar, S.; Mukhopadhyay, S. Pencil shell matrix based image steganography with elevated embedding capacity. *J. Inf. Secur. Appl.* **2021**, *62*, 102955. [CrossRef]
2. Chen, T.H.; Yan, J.Y. Enhanced Steganography for High Dynamic Range Images with Improved Security and Capacity. *Appl. Sci.* **2023**, *13*, 8865. [CrossRef]
3. Tao, F.; Cao, C.; Li, H.; Zou, B.; Wang, L.; Sun, J. Adversarial Attack for Deep Steganography Based on Surrogate Training and Knowledge Diffusion. *Appl. Sci.* **2023**, *13*, 6588. [CrossRef]
4. Chang, C.C.; Liu, Y.; Nguyen, T.S. A novel turtle shell based scheme for data hiding. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, 27–29 August 2014; pp. 89–93. [CrossRef]
5. Kurup, S.; Rodrigues, A.; Bhise, A. Data hiding scheme based on octagon shaped shell. In Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 10–13 August 2015; pp. 1982–1986. [CrossRef]
6. Liu, L.; Chang, C.C.; Wang, A. Data hiding based on extended turtle shell matrix construction method. *Multimed. Tools Appl.* **2017**, *76*, 12233–12250. [CrossRef]
7. Xie, X.Z.; Chang, C.C. Hiding data in dual images based on turtle shell matrix with high embedding capacity and reversibility. *Multimed. Tools Appl.* **2021**, *80*, 36567–36584. [CrossRef]
8. Mukherjee, S.; Mukhopadhyay, S.; Sarkar, S. A shell-matrix-based image steganography technique for multimedia security and covert communication. *Innov. Syst. Softw. Eng.* **2022**. [CrossRef]
9. Mukherjee, S.; Sarkar, S.; Mukhopadhyay, S. Octagon Shell Based Image Steganography for Avoiding Human Visual System with Lower Computational Time. In Proceedings of the 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 21–22 April 2022; pp. 1–5. [CrossRef]

10. Abdullatif, F.A.; Abdullatif, A.A.; Taha, N.A. Data hiding using integer lifting wavelet transform and DNA computing. *Period. Eng. Nat. Sci.* **2020**, *8*, 58–66.
11. Mukherjee, S.; Sarkar, S.; Mukhopadhyay, S. An Image Steganography Technique Based on Fake DNA Sequence Construction. In Proceedings of the International Joint Conference on Advances in Computational Intelligence: IJCACI 2021, New Delhi, India and Dhaka, Bangladesh Jointly, 23–24 October 2021; pp. 613–621. [CrossRef]
12. Lee, C.F.; Chang, C.C.; Li, G.L. A Data Hiding Scheme Based on Turtle-shell for AMBTC Compressed Images. *KSII Trans. Internet Inf. Syst.* **2020**, *14*, 2554–2575. [CrossRef]
13. Horng, J.H.; Chang, C.C.; Li, G.L. Steganography using quotient value differencing and LSB substitution for AMBTC compressed images. *IEEE Access* **2020**, *8*, 129347–129358. [CrossRef]
14. USCID Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 14 July 2023).
15. European Bioinformatics Institute. Available online: http://www.ebi.ac.uk/ (accessed on 15 July 2023).
16. NCBI Database. Available online: http://www.ncbi.nlm.nih.gov/ (accessed on 15 July 2023).
17. Bandyopadhyay, S.; Sarkar, S.; Mukherjee, S.; Mukhopadhyay, S. Pixel Interpolation Followed by Prediction Error Expansion-Based Reversible Information Hiding Algorithm for Securing Healthcare Data. In *Proceedings of the Frontiers of ICT in Healthcare: Proceedings of EAIT*; Kolkata, India, 30–31 March 2022, pp. 375–385. [CrossRef]
18. Mukherjee, S.; Sarkar, S.; Mukhopadhyay, S. A LSB substitution-based steganography technique using DNA computing for colour images. In Proceedings of the International Conference on Innovations in Software Architecture and Computational Systems: ISACS 2021, Kolkata, India, 2–3 April 2021; pp. 109–117. [CrossRef]
19. Bandyopadhyay, S.; Mukherjee, S.; Jana, B.; Chowdhuri, P. A Data Hiding Technique Based on QR Code Decomposition in Transform Domain. In Proceedings of the International Conference on Frontiers in Computing and Systems: COMSYS 2021, Shillong, India, 29 September–1 October 2021; pp. 425–432. [CrossRef]