PASCAL Journal of Computer Science and Informatics
https://jurnal.devitara.or.id/index.php/komputer
E-ISSN: 3047-5074 Volume 1 Nomor 1 Tahun 2023

Layered Data Security Using Affine Cipher and Pixel Value Differencing Steganography

Rivalri Kristianto Hondro
Universitas Budi Darma, Medan, Indonesia

ARTICLE INFO

Keywords:
affine cipher;
pixel value differencing;
steganography;
cryptography;
data security

Email:
rivalryhondro@gmail.com

ABSTRACT

This study presents a layered data-security design that combines Affine Cipher encryption with Pixel Value Differencing (PVD) image steganography. The first layer transforms plaintext into ciphertext using a monoalphabetic affine transformation, while the second layer conceals the ciphertext in neighboring image pixels according to local pixel differences. The method is reconstructed as a consistent Affine-PVD workflow and verified through deterministic worked examples rather than unsupported attack-success claims. Using the uppercase alphabet with keys a = 5 and b = 8, the plaintext "DATA" is transformed into "XIZI" and correctly recovered with the modular inverse. In the PVD verification, the pixel pair (100, 108) embeds the three-bit sequence 101 by changing the difference from 8 to 13, producing a valid modified pair (98, 111); extraction recovers the same bit sequence. These results confirm algorithmic reversibility of the two stages. The combined approach provides confidentiality and concealment as separate layers, but Affine Cipher remains a classical cipher and PVD is susceptible to steganalysis. Therefore, the design is appropriate as a prototype or instructional security model rather than a substitute for modern cryptographic protection.

Copyright © 2023 PASCAL.
All rights reserved is Licensed under a Creative Commons Attribution- NonCommercial 4.0 International License (CC BY-NC 4.0)

INTRODUCTION

Protecting confidential data requires more than preventing unauthorized reading. In many communication scenarios, the existence of a secret message may itself attract attention. Cryptography addresses message confidentiality by transforming readable plaintext into ciphertext, whereas steganography conceals the presence of the message inside another medium. Combining the two techniques therefore creates two distinct protection layers: a message must first be detected or extracted from the cover medium and then correctly decrypted before its original content becomes available (Sahu & Swain, 2016; Alhomoud, 2021).

Affine Cipher is a classical monoalphabetic substitution cipher that maps each plaintext symbol through multiplication and addition under modular arithmetic. It is simple to implement and useful for demonstrating key-based encryption, but its deterministic substitution structure does not provide the security expected from modern cryptographic systems. Prior studies have therefore combined Affine Cipher with other cryptographic mechanisms to reduce its structural weaknesses or to add additional protection layers (Rachmawati & Candra, 2015; Siregar, 2019; Khairani et al., 2021; Diana, 2022).

Pixel Value Differencing (PVD), introduced by Wu and Tsai (2003), is a spatial-domain steganographic method that embeds more secret bits in high-contrast regions and fewer bits in smooth regions. The embedding capacity is determined from the difference between neighboring pixels. Subsequent studies have examined weaknesses in the pixel-difference histogram, combined PVD with least-significant-bit substitution, and proposed adaptive or modulus-based variants to improve capacity and visual quality (Zhang & Wang, 2004; Wu et al., 2005; Wang et al., 2008; Khodaei & Faez, 2012).

This study integrates Affine Cipher and PVD in a single security workflow for text messages hidden in digital images. The research contribution is not a claim that the combination is cryptographically unbreakable; instead, it provides a consistent implementation model, a reversible transformation sequence, and an analysis of the security properties and limitations of each layer. This framing is important because classical encryption and spatial-domain steganography can add complexity for an attacker but cannot replace modern authenticated encryption when strong production security is required.

PASCAL Journal of Computer Science and Informatics
https://jurnal.devitara.or.id/index.php/komputer
E-ISSN: 3047-5074 Volume 1 Nomor 1 Tahun 2023

METHOD

This study uses a prototype-oriented design to develop a web-based text security system combining Affine Cipher and Pixel Value Differencing (PVD). The process consists of encryption, binary conversion, PVD embedding, extraction, and decryption.

Affine Cipher

Let x denote the numerical value of a plaintext symbol in an alphabet of size m. Affine encryption uses two keys, a and b, where gcd(a,m)=1. The encryption and decryption functions are:

$$E(x) = (a\,x + b) \bmod m$$

$$D(y) = a^{-1}\,(y - b) \bmod m$$

The multiplicative inverse a^{-1} exists only when a is relatively prime to m. For the worked verification, uppercase letters A-Z are mapped to 0-25, m = 26, a = 5, and b = 8. The inverse of 5 modulo 26 is 21 because (5 × 21) mod 26 = 1. The web implementation may extend the symbol domain to printable ASCII, but the same coprimality requirement must be preserved (Menezes et al., 1996; Munir, 2019).

Pixel Value Differencing

PVD embeds the binary ciphertext into pairs of neighboring pixels. The pixel difference \(d=|p_1-p_2|\) determines the embedding range. The number of embedded bits is:

$$n = \lfloor \log_2(w_k) \rfloor$$

where \(w_k\) is the range width. The pixel pair is then adjusted to represent the target difference while maintaining valid pixel values (Wu & Tsai, 2003).

Integrated Workflow

Table 1. Integrated Affine-PVD Security Workflow

Stage	Input	Output
1. Encryption	Plaintext + Affine keys	Ciphertext
2. Bit conversion	Ciphertext	Binary ciphertext stream
3. PVD embedding	Binary ciphertext + cover image	Stego-image
4. PVD extraction	Stego-image	Binary ciphertext stream
5. Reconstruction	Extracted bits	Ciphertext
6. Decryption	Ciphertext + Affine keys	Recovered plaintext

The intended security logic is layered. PVD hides the ciphertext rather than the readable plaintext, so successful steganographic extraction does not immediately reveal the original message. Conversely, knowledge of the Affine keys is not sufficient unless the ciphertext is first obtained from the stego-image. The receiver therefore performs the reverse order: extraction followed by decryption.

Verification Criteria

Correctness is evaluated through round-trip testing: Affine decryption must recover the original plaintext, PVD extraction must reproduce the embedded ciphertext bits, and the complete process must preserve the ciphertext. Future evaluation may use MSE, PSNR, and embedding capacity (bits per pixel). Lossless formats such as PNG or BMP are recommended for testing.

RESULTS AND DISCUSSION

Affine Cipher Verification

Using the test plaintext “DATA”, the numerical representation is D=3, A=0, T=19, and A=0. With a=5 and b=8, the encrypted values are 23, 8, 25, and 8, which correspond to the ciphertext “XIZI”. Applying the inverse key a^{-1}=21 returns the original values 3, 0, 19, and 0. The worked example therefore verifies the reversibility of the Affine transformation for a valid key pair.

Table 2. Worked Affine Cipher Verification

Plain	x	E(x)	Cipher	Recovered

D	3	23	X	D
A	0	8	I	A
T	19	25	Z	T
A	0	8	I	A

The result confirms computational correctness, but it should not be interpreted as evidence of modern cryptographic strength. Affine Cipher is monoalphabetic and preserves substitution regularities across repeated symbols. The security benefit of the proposed design therefore comes primarily from layering and concealment, not from treating Affine Cipher as a contemporary high-security cipher. Studies that combine Affine Cipher with other mechanisms similarly indicate that additional transformations are used to compensate for the simplicity of the basic affine substitution (Siregar, 2019; Khairani et al., 2021; Diana, 2022).

PVD Embedding and Extraction Verification

A deterministic pixel-pair example is used to verify the PVD arithmetic. Consider the neighboring grayscale pixels (100,108), giving d=8. The difference falls in the range [8,15], whose width is 8; therefore n=3 secret bits can be embedded. For secret bits 101, the decimal value is 5 and the target difference is d′=8+5=13. One valid adjustment is (98,111), whose absolute difference is 13 and whose values remain in the valid 0-255 interval.

Table 3. Worked PVD Verification

Original Pair	d	Range	Bits	Stego Pair	Extracted
(100,108)	8	[8,15]	101	(98,111)	101

During extraction, the receiver recomputes the stego difference 13, identifies the same range [8,15], and calculates 13-8=5. The value 5 represented with three bits is 101, reproducing the embedded segment. This confirms the basic reversible property required by the PVD stage. In a full image, the process is repeated across successive pixel pairs until all ciphertext bits are embedded or the image capacity is exhausted.

Layered Security Analysis

The combined design provides two different forms of protection. Encryption changes the semantic content of the message, while steganography changes its visibility. If an observer only sees the stego-image, the presence of the ciphertext is not explicit. If the hidden payload is extracted without the Affine key, the extracted data remains ciphertext. This layered structure is conceptually stronger than transmitting plaintext hidden directly in an image because compromise of one layer does not automatically reveal readable content.

However, neither layer should be overstated. The original PVD method is vulnerable to statistical analysis of pixel-difference histograms, and several later methods were proposed specifically to improve its security, capacity, or distortion characteristics (Zhang & Wang, 2004; Wu et al., 2005; Wang et al., 2008; Khodaei & Faez, 2012; Khodaei et al., 2016). Likewise, Affine Cipher is appropriate for classical-cryptography demonstrations but is not resistant to modern cryptanalysis when used alone. For operational systems that require strong confidentiality, modern authenticated encryption should protect the message before optional steganographic concealment.

Implementation Considerations and Limitations

Table 4. Implementation Considerations

Aspect	Recommended Practice	Reason
Affine key	Require gcd(a,m)=1 and protect both keys	Ensures decryptability and prevents trivial key exposure.
Cover format	Prefer PNG/BMP or avoid JPEG recompression	PVD depends on preserved pixel values.
Capacity	Check available pixel-pair capacity before embedding	Prevents incomplete payload insertion.
Pixel bounds	Reject or readjust values outside 0-255	Avoids overflow/underflow artifacts.

Evaluation	Report MSE, PSNR, payload, and extraction accuracy	Separates correctness from visual quality.
Production security	Use modern encryption before steganography	Affine Cipher is a classical educational cipher.

The main limitation of the present study is the absence of a valid experimental dataset containing original cover images, stego-images, payload sizes, PSNR/MSE values, and extraction trials for the Affine-PVD combination. Consequently, this article reports algorithmic verification rather than fabricated quantitative performance results. A subsequent experiment should use multiple lossless test images with different texture characteristics, several payload sizes, repeated extraction tests, and comparison with baseline PVD. Such an evaluation would allow the capacity-imperceptibility trade-off to be quantified objectively.

CONCLUSION

The integration of Affine Cipher and Pixel Value Differencing provides a coherent two-layer model for protecting text data. Affine Cipher transforms the readable message into ciphertext, while PVD conceals the ciphertext within neighboring image pixels according to local intensity differences. Deterministic verification confirms that both stages are reversible when valid parameters are used: the example plaintext “DATA” is encrypted to “XIZI” and recovered correctly, while the PVD example embeds and extracts the bit sequence 101 without leaving the valid pixel range. The combination improves concealment compared with transmitting the ciphertext openly, but it does not establish modern cryptographic security. Affine Cipher remains vulnerable as a classical substitution cipher, and PVD can be targeted by steganalysis. Future work should replace the encryption layer with modern authenticated encryption, retain steganography as an optional concealment layer, and perform quantitative testing with PSNR, MSE, payload capacity, extraction accuracy, and steganalysis resistance.

REFERENCES

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6

Zhang, X., & Wang, S. (2004). Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters, 25(3), 331-339. https://doi.org/10.1016/j.patrec.2003.10.014

Wu, H.-C., Wu, N.-I., Tsai, C.-S., & Hwang, M.-S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings - Vision, Image and Signal Processing, 152(5), 611-615. https://doi.org/10.1049/ip-vis:20059022

Wang, C.-M., Wu, N.-I., Tsai, C.-S., & Hwang, M.-S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software, 81(1), 150-158. https://doi.org/10.1016/j.jss.2007.01.049

Yang, C.-H., Weng, C.-Y., Wang, S.-J., & Sun, H.-M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transactions on Information Forensics and Security, 3(3), 488-497. https://doi.org/10.1109/TIFS.2008.926097

Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image Processing, 6(6), 677-686. https://doi.org/10.1049/iet-ipr.2011.0059

Rachmawati, D., & Candra, A. (2015). Implementasi kombinasi Caesar dan Affine Cipher untuk keamanan data teks. JEPIN (Jurnal Edukasi dan Penelitian Informatika), 1(2). https://doi.org/10.26418/jp.v1i2.12587

Sahu, A. K., & Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. Indonesian Journal of Electrical Engineering and Computer Science, 2(3), 712-719. https://doi.org/10.11591/ijeecs.v2.i3.pp712-719

Khodaei, M., Sadeghi Bigham, B., & Faez, K. (2016). Adaptive data hiding, using pixel-value-differencing and LSB substitution. Cybernetics and Systems, 47(8), 617-628. https://doi.org/10.1080/01969722.2016.1214459

Siregar, I. M. (2019). Penerapan algoritma Affine Cipher dan algoritma Columnar Transposition dalam keamanan teks. Jurnal Informatika Kaputama, 3(1), 6-12. https://doi.org/10.59697/jik.v3i1.391

Munir, R. (2019). Kriptografi (Edisi Kedua). Informatika Bandung.

Alhomoud, A. M. (2021). Image steganography in spatial domain: Current status, techniques, and trends. Intelligent Automation & Soft Computing, 27(1), 69-88. https://doi.org/10.32604/iasc.2021.014773

Khairani, T., Santoso, K. A., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean monoalphabetic menggunakan Affine Cipher dengan kunci Diffie-Hellman. PRISMA, Prosiding Seminar Nasional Matematika, 4, 553-559.

Alade, O. M., Amusan, E. A., Adedeji, O. T., & Alo, O. O. (2021). Image steganography using Pixel Value Differencing (PVD) technique based on Firefly Algorithm. Journal of Scientific Research and Reports, 27(7), 80-86. https://doi.org/10.9734/jsrr/2021/v27i730414

Diana, I. N. (2022). Algoritma super enkripsi (Affine Cipher dan Cipher Transposisi Grup Simetri) untuk mengamankan pesan teks. KUBIK: Jurnal Publikasi Ilmiah Matematika, 7(1). https://doi.org/10.15575/kubik.v7i1.17419