Secure Cryptographic Scheme based on Dual of Generalized Reed-Muller (GRM) Codes for Image Encryption

Vipin Yadav, Department of Applied Sciences, the North Cap University, Gurugram, India,
Seema Thakran, Department of Applied Sciences, the North Cap University, Gurugram, India,
Anshu Malhotra , Dept. of Computer Sciences , K.R. Mangalam University, Gurugram, India,
Hukum Singh, Department of Applied Sciences, the North Cap University, Gurugram, India,

Abstract
Cryptosystems using error-correcting codes offer a powerful combination of security and reliability. In this paper, a secure cryptographic approach over noisy channels applying Dual of Generalized Reed-Muller (DGRM) codes is proposed. The implementation of these codes enables the localization and correction of errors. It enhances both of the security and efficiency in the channel. In the scheme, a binary image is encoded using DGRM codes which add redundancy bits to it and increase the error-resistant quality. The private key produced during the encryption is utilized in the decryption system to retrieve the input image. System performance is tested by evaluating the Mean-squared error (MSE), Peak signal to-noise ratio (PSNR), SSIM and correlations coefficients. The Robustness of the scheme is tested against basic attacks (i.e. CPA, KPA). The proposed scheme is digitally implemented using MATLAB (2024a).

Keywords
Reed-Muller codes; hamming distance; Parity check Matrix; Generalized Reed-Muller codes (GRM); Dual of Generalized Reed-Muller codes (DGRM).

1 Introduction

Error-correcting codes (ECCs) such as Reed-Muller are employed in a variety of fields such as information and communication system. They were created for digital storage systems and wireless communication systems over noisy channels. These codes were used for space communication in theMariner9 spacecraft, are widespread in coding theory textbooks and research publications [1,2]. There are number of generalizations of Reed-Muller codes over GF (q) have been developed in recent years [3,4]. In literature, we have focused on the generalization which was introduced by Dass and Muttoo in 1980, named as GRM codes of order $\square + (\square + 1)\square$, $\square$[5]. B.K Dass and S.K Wasan also presented the weight distribution of the Dual of Generalized -Reed-Muller codes of order $\square + (\square + 1)\square$, $\square$. V. Tyagi and S. Rani [6-7] further extended their research on Dual of GRM codes and established new construction using multiple of DGRM codes. Structural and error correcting capabilities of these codes makes feasible to use them in image encryption scheme [8].
Many scholars have attempted to integrate error correction and encryption into a single

DOI: https://doi.org/10.5281/zenodo.15088877

device in order to examine the trade-off between these two features. For instance, In 1978, McEliece used Goppa code [9] to construct public-key cryptosystem which can encrypt data quickly.In 1984, Rao and Nam[10] introduced the Rao–Nam scheme, named as private-key algebraic-coded cryptosystem (PRAC) after incorporating basic algebraic BCH code.Nieder-reiter et.al.[11] developed a novel public-key cryptosystem in 1986, which wasnamedas N- public key.In 2006, Mathur and Narayan et al [12] raised the high diffusion (HD) cipher which is based on the SPN (Substitution-Permutation network) structure. Encryption and error correction are combined in this method, which diffuses the muddled message using HD codes. An approach utilizing Interleaver and LDPC code was introduced in 2006 by Xiao et. al. [13].

In 2010, Adamo et al. [14] proposed a scheme named ECBC which combines encryption and error correction in one-step.In 2013, Cankaya et al. [15] applied the linear error correction (LEC) code, permutation and compression to the cryptosystem. In 2014, Ning et al. [16] presented a scheme used in satellite communications which incorporates AES and LDPC.In 2015,Yao et al. [17] raised a JEEC scheme based on chaos and Turbo code. They modified the scheme proposed by Zhang and Mao [18] and encrypted the outputs of the chaotic convolutional coder in order to enhance the security. The level of efficiency was exceedingly low, and the security was obtained at the expense of error correction capability

In this paper, we have focused on developing a error correction encryption scheme based on Dual of GRM codes (DGRM). To the best of the Author knowledge, no study have been reported which have used DGRM codes in image encryption.The paper is structured into four Sections: In Section 1, we have mentioned all the theoretical concepts used in the paper. Section 2, contains the proposed scheme. Simulation results are given in Section 3 and last Section includes the concluding segment.

2. Theoretical background

Generalized Reed-Muller Codes of order $r + (r + 1)_{m,s}$

In 1982, Dass and Muttoo, obtained a new class of generalized Reed–Muller codes, known as GRM codes of order $r + (r + 1)_{m,s}$ by extending/shortening a r^{th}-order of RM codes [56].

Definition: A GRM code of order $r + (r + 1)_{m,s}$is generated by basis vector$\{v_0, v_1, v_2 - --, v_m\}$ and vectors product of $v_0, v_1, v_2 - --, v_m$ taken r or fewer at a timealong with some s vector products $(1 \leq s < \binom{m}{r+1})$ of these vectors taken $(r + 1)$ at a time.

Parameters of GRM codes:

Code length: $n = 2^m$ (1)

Dimension: $k = 1 + \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \ldots \binom{m}{r} + s$; *where* $1 \leq s < \binom{m}{r+1}$.(2)

Minimum distance: $d_{min} = 2^{m-r-1}$(3)

Dual of Generalized Reed-Muller (DGRM) Codes

The dual of code is a linear code denoted by $C^{\perp}$. Wasan and Games (1982) have shown that the minimum distance of GRM codes of order $r + (r + 1)_{m,s}$ is$2^{m-(r+1)}$. Dual of

DOI: https://doi.org/10.5281/zenodo.15088877

GRM code of order □ + + 1)m,s is (□
given as (□ − □ − 2) +(□ − □ − 1m,s′)
where□′ = (m m−r−1).

3 The Proposed Cryptosystem

3.1 Permutation function

We define a functionσ_s: $(\mathbb{Z}_2^n)^k \rightarrow (\mathbb{Z}_2^n)^k$for every matrixV∈ $(\mathbb{Z}_2^n)^k$specified by the permutation key□ where $(\mathbb{Z}_{(x,y)}^n)^k$is □∈
denoted as matrix:

$\sigma_s(V) = S * V_1$ (4)

3.2 Encryption Steps

Step 1: Initially, the input image I of order 250*250 is multiplied with Private Key σ_s which results as P.

$P = \sigma_s(I(x, y))$; P = matrix of order 250*250
(5)

Step 2: P is encoded using DGRM encoder of order 256*512. DGRM encoder adds redundancy to the data and produces the matrix W. Mathematically represented as,

W = P × DGRM; (W is rectangular matrix of order 250*512) (6)

Step 3: Encoded data is transmitted through a noisy channel and random error is added using error matrix E_r.

$E = W + E_r$; E is the encrypted image of order 250*512

The encryption process can be represented as follows, 6

$E = (\sigma_s(I) \times DGRM) + E_r$; (7)

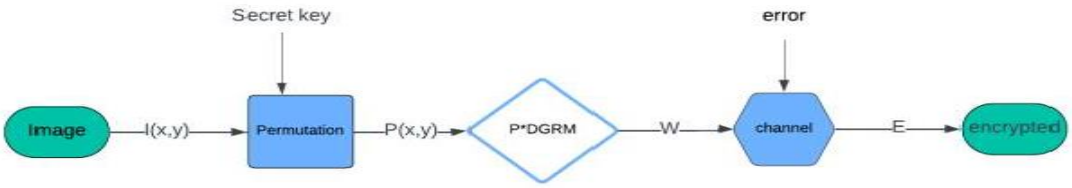


Fig. 1 Flowchart of encryption process

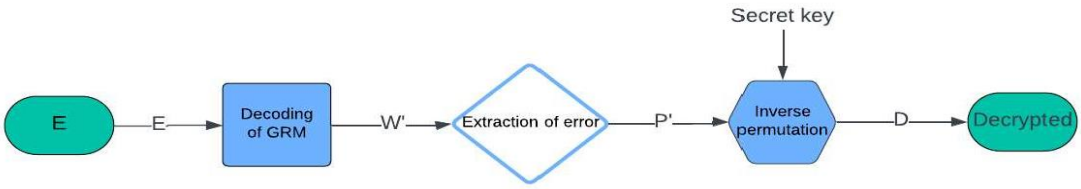
3.2 Decryption Steps

Step 1: The final output of the encryption process, E, serves as input for decoding process. Initially E, is decoded and error is extracted using decoding of DGRM codes

Step 2 : Inverse permutation function $\sigma_s'$of permutation key σ_s is computed over □' and decrypted image D is recovered

$D = \sigma_s'(□')$ (8)

Fig. 2 Flowchart of decryption process



DOI: https://doi.org/10.5281/zenodo.15088877

4 Simulation results

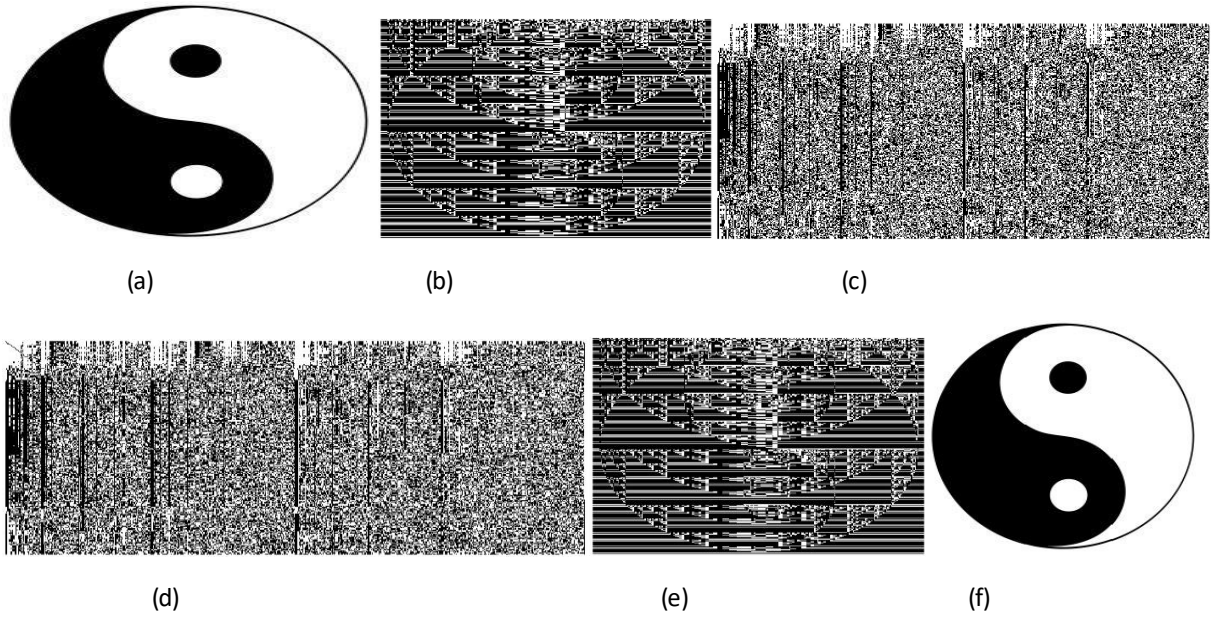


Fig 3: A Input Image: b image after key: **c** Image after DGRM code: **d** image to receiver with error: **e** decoded image by DGRM decoder: f decrypted image after key

4.1 Performance Analysis

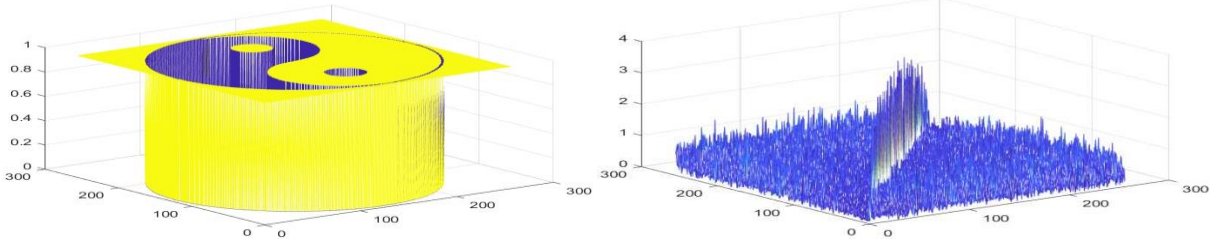
Table 1. Quality Assessment Techniques

Image	MSE	PSNR	SSIM	CC
LENA	0	∞	1	1
CAT	0	∞	1	1
LOGO	0	∞	1	1

4.2 Statistical Analysis

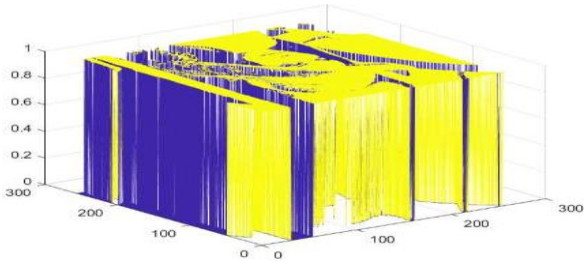
3d plot Analysis

3d plot of encrypted images reflects the security of the cryptosystem. In this scheme, we have encrypted two different images and could not find the difference between the encrypted images of both Input images. so, it is not possible to get the information of the input image by analysis the 3d plot of the Encrypted image as it is same for both of the image.

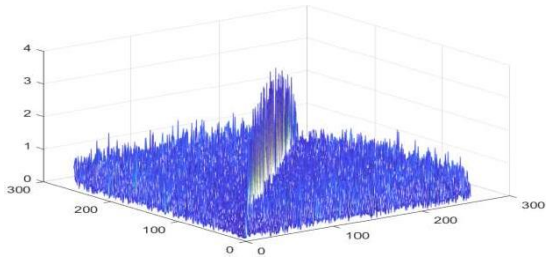


(a) **(c)**

DOI: https://doi.org/10.5281/zenodo.15088877



(b)



(d)

Fig.4. (a) 3d plot of logo binary image, (b) Lena image plot, (c) 3d plot of encrypted logo image and (d) plot of encrypted Lena image

DGRM code error correcting capabilities:
We used DGRM codes constructed by shortening the r^th- Reed-Muller codes. In our scheme, we used m=9,r=4,and s=0 generates DGRM encoder matrix of order 256*512. Weight of the code is 2^(9-4)=32 which can correct up to 15 errors.

4.3 Robustness analysis

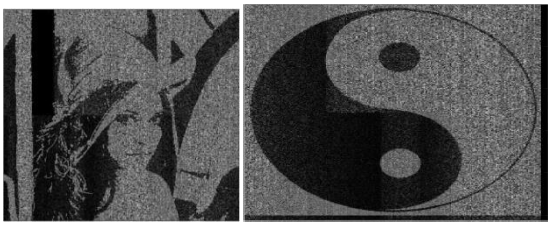
A system is secured and robust if it is resistant to attacks. The proposed cryptosystem is tested against contamination attacks and classical cryptographic attacks (CPA, QPA) and found to be robust.

Contamination attack analysis

The scheme is highly secured and has been tested against noise contamination attack. To verify this, we have done the analysis on noise attack with Gaussian noise. The encrypted image after adding the noise is as follows:

$$E_0' = E_0 (1 + kG), \quad (9)$$

Where E_0' and E_0 are contaminated encrypted image and encrypted image respectively. G denotes the Gaussian random noise with zero mean and 1 variance, k denotes the coefficient of strength of the noise. In our analysis, encrypted image is contaminated with values of k = 0.3 and 0.5, The corresponding decrypted image is shown in fig 5.

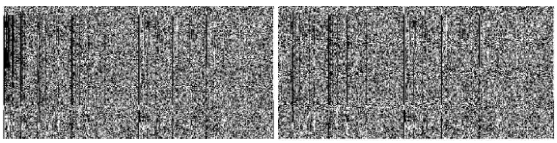


(a) (b)

Fig.5 (a) and (b) represents the decrypted image recovered from noise contaminated image with values of k= 0.3 and k=0.5 respectively.

Plaintext attacks

In the proposed cryptosystem, we have checked the robustness of our scheme against plaintext attacks, i.e. known plaintext attacks (KPA) and chosen plaintext attacks (CPA). To check the robustness against these attacks, encrypted image of Lena and Logo is deciphered with wrong (exchanged) private keys. The results are shown in Fig. 6, which proves the robustness of the scheme against the aforementioned attacks.



(a) **(b)**

DOI: https://doi.org/10.5281/zenodo.15088877

Fig.6(a) represent the decipher image of Lena and (b) represents the decipher image of Logo retrieved by their exchanged private keys.

5 Conclusions

The proposed cryptographic scheme offers a promising secured system for enhancing data security based on DGRM codes for image encryption. The capabilities and efficient encoding techniques of DGRM codes provides robust cryptographic scheme to enhance the security and confidentiality. The MSE and PSNR values also verify the effectiveness and robustness of the scheme.The scheme is tested against basic attacks chosen plain-text attacks (CPA) and known plain-text attacks (KPA).According to experimental results, our technology can fix big, corrupted blocks in photos, something that other previously published methods have not been able to do.

References

1. Kamble, A. J., & Venkatesh, T. (2015). Some Applications of Error-correcting Codes. Journal of Computer and Mathematical Sciences, 6(11), 604-611.
2. Kudekar, S., Kumar, S., Mondelli, M., Pfister, H. D., Şaşoğlu, E., &Urbanke, R. (2016, June). Reed-Muller codes achieve capacity on erasure channels. In Proceedings of the forty-eighth annual ACM symposium on Theory of Computing (pp. 658-669).
3. Delsarte, P., Goethals, J. M., & Mac Williams, F. J. (1970). On generalized reedmuller codes and their relatives. Information and control, 16(5), 403-442.
4. Ding, P., & Key, J. D. (2000). Minimum-weight codewords as generators of generalized Reed-Muller codes. IEEE Transactions on Information Theory, 46(6), 2152-2158.
5. Dass, B.K., Wasan,S.K.(1983).On codes of order r+(r+1), International journal of electronics,pp.471-475.
6. Tyagi, V., & Rani, S. (2012). New construction of GRM codes. Asian-European Journal of Mathematics, 5(01), 1250012.
7. Tyagi, V., & Rani, S. (2012). Recursive matrix method for GRM and DGRM codes. International Electronic Journal of Pure and Applied Mathematics, 4(4), 263-270.
8. Dumer, I., &Shabunov, K. (2006). Recursive error correction for general Reed–Muller codes. Discrete Applied Mathematics, 154(2), 253-269.
9. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic. Coding Thv, 4244(1978), 114-116.
10. Rao, T. R., & Nam, K. H. (1986, August). Private-key algebraic-coded cryptosystems. In Conference on the Theory and Application of Cryptographic Techniques (pp. 35-48). Berlin, Heidelberg: Springer Berlin Heidelberg.
11. Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inform. Theory, 15(2), 157-166..
12. Mathur, C. N., Narayan, K., & Subbalakshmi, K. P. (2007). On the design of error-correcting ciphers. EURASIP Journal on Wireless Communications and Networking, 2006, 1-12.
13. Xiao, Y., Zhao, Y., & Lee, M. H. (2006, November). Encrypting LDPC-codec. In 2006 8th international Conference on Signal Processing (Vol. 3). IEEE.

DOI: https://doi.org/10.5281/zenodo.15088877

14. Adamo, O., Fu, S., & Varanasi, M. R. (2010, December). Physical layer error correction based cipher. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 (pp. 1-5). IEEE.
15. Cankaya, E. C., Nair, S., &Cankaya, H. C. (2013). Applying error correction codes to achieve security and dependability. Computer Standards & Interfaces, 35(1), 78-86.
16. Ning, L., Kanfeng, L., Wenliang, L., & Zhongliang, D. (2014). A joint encryption and error correction method used in satellite communications. China communications, 11(3), 70-79.
17. Yao, J., Liu, J., & Yang, Y. (2015). Joint encryption and error correction technical research applied an efficient turbo code. International Journal of Security and Its Applications, 9(10), 31-46.
18. Zhang, W., & Mao, Q. (2012). Error-correcting and encryption joint coding scheme based on turbo code. Radio Commun. Technol., 38, 29-32.
19. Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed-Muller codes.
20. Gligoroski, D., Knapskog, S. J., & Andova, S. (2006, June). Crypt coding-Encryption and Error-Correction Coding in a Single Step. In Security and Management (pp. 145-151).

DOI: https://doi.org/10.5281/zenodo.15088877