International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume 15 Issue 02 Year 2023

Recognition of the Integrity of Chic China Aesthetic Elements Based on Computer Vision Technology

Meijun Lu

Ph.D Candidate, The Design School, Faculty of Innovation and Technology, Taylor's University Lakeside Campus, Selangor，47500, Malaysia

myra1009@163.com

Charles Sharma Naidu*

Doctor, VORTEX XR Lab, The Design School, Faculty of Innovation and Technology, Taylor's University Lakeside Campus, Selangor，47500, Malaysia

charles.sharma@taylors.edu.my

Yichuan Di

Assistant Professor, School of New Media Art and Design, Beihang University, Beijing, China

zxbbzdyc@buaa.edu.cn

Article History

Received: 6 June 2023
Revised: 10 July 2023
Accepted: 21 August 2023

Abstract

Recent trends in the fashion industry indicate that China Chic (CC) has emerged as an integral part of the Chinese lifestyle. The fashion industry in recent years was dominated by foreign brands or luxury brands because of the economic conditions and the failure to produce iconic designs by the domestic fashion industry. Recent years have witnessed the genesis of China-chic brands that began to produce original designs with a traditional touch to modern outfits. As a result of which, many international fashion elements were integrated into their clothes and accessories. However, many types of security attacks are pronounced on these elements, which will degrade their market value. This work proposes a computer vision-based defrauding model that relies on a Siamese-based Convolutional Neural Network (S-CNN) to detect counterfeited and fake products. This is done by injecting adversarial attacks on Simplified Graph Convolutional Networks (SGCN) that effectively misclassify the Adversarial Images (AdI), which are created by the Improved Fast Gradient Sign Method (I-FGSM). The training phase of the proposed model is performed using the ImageNet dataset augmented with AdI. The testing is done using the custom dataset of the CC elements, which showed a 6% improvement over the S-CNN, which is a breakthrough in preserving the integrity of the CC elements.

Keywords: CC, Computer Vision, Fast Gradient Sign Method, Simplified Graph Convolutional Networks, Adversarial Attack, Integrity

1. Introduction

China is generally perceived as the world's factory as the early stage of economic development was mainly due to the availability of low-cost labour, which served as a competitive edge over the other countries [1]. The Chinese state has refined the country's international trade policy, which brought economic reforms primarily centred on innovations in design, manufacturing, technology, business models, and management along the production line [2]. This forced the local producers to shift their attention to producing goods of superior quality. Consumers across the world started to recognize the market value of Chinese goods, which eventually transformed the notion of the tagline from "Made in China" to "Designed in China" [3]. This has indeed raised the cultural confidence in the minds of the citizens of China, which are expected to dominate the global market [4].

For the last two decades, China has witnessed an inclining trend of the sense and notion of national pride, which is mainly due to its financial growth and dominance in international politics [5]. CC is a fresh phrase that best describes the latest emerging trend of China-centric design. The entomology of this word is similar to "Bristyle", which incorporates the native cultural elements and the latest trends in the fashion industry [6]. But recent times witnessed that this CC has expanded its horizons, including fashion, accessories, cosmetics, technology, automobiles, and even in retail sales. It has already started to manifest the Chinese people's motivation to revive their ancient traditional heritage in a more modern context, thereby reflecting the pride in their nation's identity [7].

As the China-chic has now become an inseparable part of China's fashion industry, it has now aroused the economic development of the traditional industries. The country's fashion designers and people were mostly focused on relying on foreign fashion brands and luxury brands, some foreign fashion brands or luxury brands. The reason behind this is that the Chinese contemporary fashion practitioners and fashion brands were not interested in creating iconic designs and largely focused on copying the common international designs. Unlike the previous older generations, the young people did not perceive the country as a flood-lit- poor country flooded, which is known for its fake, cheap, and sub-optimal quality products [8]. Besides its turbulence in international relations with many countries, the younger population of China does not incline to Western brands. This trend is further accelerated after the pandemic as the country has pushed itself for technological and economic self-reliance, thus creating new trends and opportunities for local Chinese brands. The improvement in the dominance of Chinese brands in the global market is shown in Figure 1.

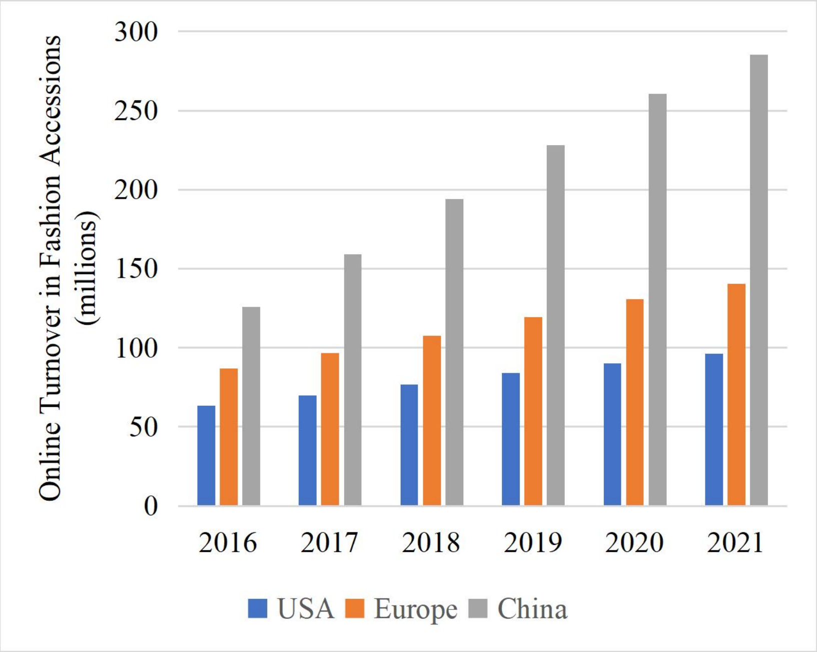

Figure 1. Increase in Sales of Fashion Accessories of Chinese Brands

In the initial days of introducing Chic Chinese elements, the world did not perceive them as unique, accurate materials and underestimated the taste of China-chic brands with very low key. The early days of China-chic brands materialized the traditional aesthetics of the country, such as the Forbidden City, Peking Opera, and other Chinese historical stories, which have local characteristics but are tedious and time-consuming. Figure 2 and Figure 3 show a few famous CC fashion design works. These local characteristics are the uniqueness that adds aesthetic appeal to the fashion elements, but the industry was dormant during its introduction. However, the yesteryears witnessed the trend that China-chic brands have started to design and manufacture their original aesthetic designs, which are inclined to their traditional values, especially in their clothing and accessories. Figure 3 shows the people's interest in purchasing local brands than renowned international brands in China. However, the fashion industry is still dominated by the flooding of foreign brands, and the trend is now changing rapidly, as the Chinese prefer Chic Chinese brands over their competitors.

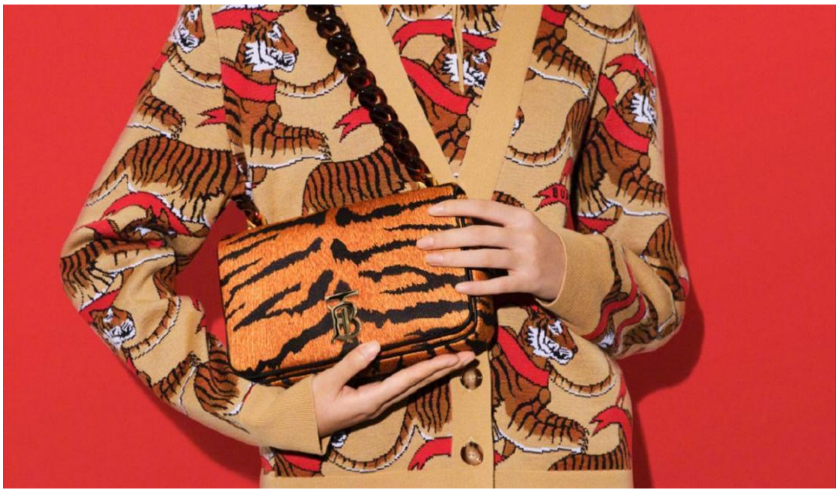

Figure 2. Chic Chinese Bag and Dress Wore by a Model

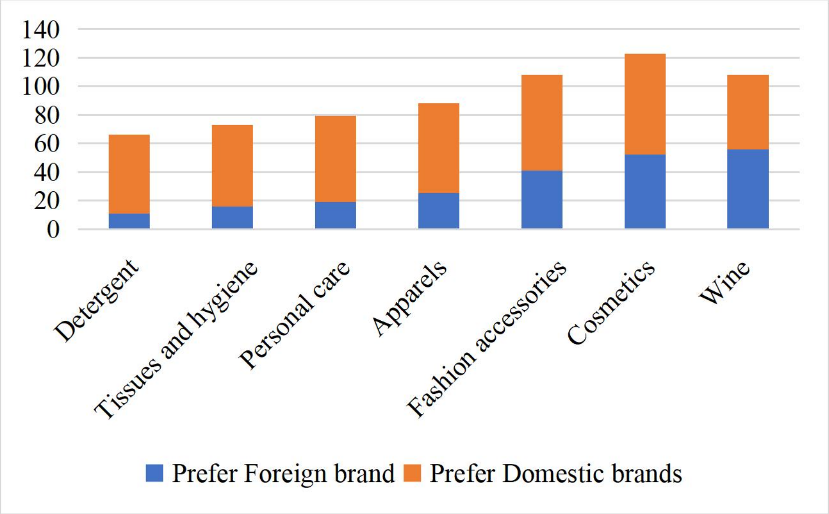

Figure 3. Comparison of Sales of Foreign and Local Brands

Thanks to the effort of fashion designers as they catalyzed this effect during the last part of the 1990s. These designers are qualified enough to intrigue the transitional designs in contemporary patterns aligning to the international standards in their fabrics and styling elements [9-10]. More innovative and creative designs are on the way, thus, paving an excellent opportunity to develop CC branding [11]. The plenishing styles by adding Chinese traditional elements has been further accelerated by international education, which has enabled versatile cultural collisions. The growth in Rap music and its aligned culture has been viewed as a game changer, which integrated culture and clothing. The celebrity effects, along with cultural integration, promote the China-chic brands. Under the guidance of these managers, numerous consumer groups are already aligned with these brands. This alignment increases their propensity to purchase and advocate for apparel from these domestic fashion labels. Through this process, the appeal of the China-chic brand is broadened, reaching a wider audience and challenging some of the pre-existing perceptions associated with China-chic style.

1.1 CC Elements

To understand the CC elements, it is important to gain knowledge about a few popular CC brands. These brands were pioneers in introducing the China design concepts with a great deal of diversity. Along with creating innovative Chic Chinese elements, these brands also integrate the patterns of integration brands with traditional touch by de-Chine seizing the designs. Some of the predominant Chic Chinese elements are described here. The study focuses on six primary categories of aesthetic elements in the context of consumer culture, specifically handbags, footwear, sportswear, furnishings, articles, and dresses [12].

1.2 LI-NING

Chinese vogue realm is clearly indicated by the increasing trend for CC after 2018, which was initiated by the domestic sportswear brand Li-Ning hit the fashion world with robust oriental-styled designs. The products were rooted in Chinese culture with a perfect blend of modern fashion. But, because of poor brand positioning, substandard design, and other market factors made the brand bear a loss of 3 billion yuan, which eventually led to the shutting off of nearly 3,000 outlets and showrooms across the country stores [13]. The company was on the verge of bankruptcy. However, the top management was quick enough to understand the challenges and re-emerged in the fashion world with better designs, quality, and modifications in being in trend. The integration of CC elements such as Su embroidery [14], red and yellow components, and the Wu dao series [15] fostered the regrowth of the company to become a trend leader brand. The brand produced sportswear with iconic materials highlighting the country's colours with a unique style and texture blended with a high concentration of Chinese features.

The application of Chinese charm with the number of classical features implanted led to and promoted the Chic Chinese culture. Some traditional patterns and trends were printed on goods, like shorts, purses, T-shirts, etc., with l futuristic as well as modern designs. Also, the intriguing yet trendy jackets were greatly inspired by the geometric printed shirts, which eventually led to the internationalization of the China-chic era in the fashion industry.

1.3 UMA WANG

This is a very popular women's clothing brand which was founded by Wang Zhi in the year 2003. This brand presents its products with China-chic fashion by integrating and introducing distinctive traditional Chinese design into international fashion trends. The prestigious collections exhibited superior fabric quality, simple lines, and a perfect amalgamation of oriental with Western styles with a mission to offer comfortable, perfect, and trendy finished garments [16]. UMA WANG [17] represents the new era of Chinese designer clothing that draws its inspiration from female painters, ballerinas, Moroccans in Mexico, knitwear, etc. The products focused mainly on the materials, intricate details, and beauty of silhouette. Hence most of the products were slender and free-flowing, similar to the costumes of the Tang Dynasty [18], which was very prosperous in the ancient Chinese era. These characteristics created an international market for Chic Chinese products.

1.4 Peacebird

This brand was established in 1997 to design and provide fashion products with a national touch. It is one of the leading companies in China that designs and manufactures readymade clothing for both men and women. It produces dresses with trendy designs with a traditional touch to it. Its products are welcomed by urban females, who strive to build a unique signature [19].

1.5 Exhibits from Dunhuang Museum

Dunhuang costume culture is another popular CC element. This creates dresses with more vigour and vitality, matching the expectations of the modern era. The exhibits at the Light of the Silk Road fostered the Dunhuang costume culture, which depicts the styles of the Early Tang Dynasty [20]. The reproduction of the aesthetic works is based on the Dunhuang murals, and they stick to maintain the shape, colour as well as composition. Modern-day principles of clothing as well as patterns, are well consumed and perceived by the designers who add an aesthetic appeal to the CC elements.

1.6 Challenges Faced by CC Aesthetics Elements

Economic growth, elevated disposable incomes, and an increase in the middle-class population have created brighter opportunities for CC goods. Despite these optimistic views, there are a few hurdles due to market and environmental changes, which greatly impact the marketing strategies of domestic CC aesthetics. A few prominent challenges are discussed here [21].

Addressing Issues of CC in the Introduction

1)Cultural Appropriation: The concerns surrounding cultural appropriation are acknowledged, and this paper explores how our proposed methodology can effectively discern authentic cultural elements, thereby mitigating unauthorized utilization and misrepresentation of cultural symbols.

The significance of maintaining the integrity of CC aesthetics is underscored, and our methodology is highlighted as a means to identify and address instances of misrepresentation pertaining to CC components.

2)Lack of Authenticity: The absence of authenticity is a topic of concern that we emphasize in relation to the preservation of the integrity of creative commons (CC) elements. This is crucial in order to guarantee their accurate portrayal within the fashion industry.

3)Insensitivity to History: Insensitivity towards history is a critical concern that we recognize in relation to the elements of cultural appropriation. We acknowledge the significance of understanding the historical context of these elements and emphasize the importance of our approach in contributing to the preservation and respectful utilization of cultural heritage.

4)Homogenization of Culture: The present discourse examines the potential of identifying authentic cultural components to foster and safeguard the diversity and distinctiveness of Chinese culture within the realm of fashion.

5)Ethical Production: The topic of ethical production is examined in relation to the fashion industry, specifically focusing on concerns regarding counterfeit products. The significance of our proposed method is underscored in promoting ethical production and consumption of CC aesthetics.

1.6.1 Issues in Intellectual Property Rights

Right from the beginning of the CC aesthetic brand building, the industry is constantly facing threats from counterfeits to trademark trolls, which fall under the violations of intellectual property. This is a potential security threat for fashion aesthetics companies, and success greatly depends on brand perception by the public. But this is greatly demolished by the flooding of fakes in the market, which is far bigger than the brand. It is evident that counterfeits degrade the brands' image and spoil the reputation of the company and its products [22]. Preserving integrity is done using various contemporary computing techniques like Computer Vision, Machine Learning, and Deep Learning [23].

1.6.2 Higher Costs

It is evident that Chinese consumers spend a very meagre amount of money on domestic products.

1.6.3 Manpower

As the trend is very new, the workers have to understand its significance, which is time-consuming. There is a high demand and acute shortage of qualified workers in this field. The quality of products and services is very important to add to the aesthetic appeal of the products, as it will directly impact the overall image of the CC brand. The problem is more intense in smaller cities that have the same market as larger cities. Companies need more hiring and training time. They are also destined to make stronger investments.

1.7 Adversarial Networks in Verifying Integrity of CC Aesthetic Elements

Chic Chinese products are niche and unique products that reflect the nation's culture, tradition, and aesthetics to the world. As the market value of these products is very high, many sub-optimal brands mimic the production and reproduction of the CC elements in an improper way, which may tarnish the originality of the aesthetic of the representative CC element. Human views on artistic works are vision partially biased, and people are generally deceived by images of fake and counterfeit products which are not authentic [24]. This problem can be brought under adversarial attacks [25]. These attacks generate adversarial examples which are fake. Nevertheless, these creations are strikingly similar to the originals, crafted with the intent to mimic them. As illustrated in Figure 4, we see the full model of the adversarial attack. Meanwhile, Table 1 presents an analysis of the

Confidentiality-Integrity-Availability aspects within the realm of information security, specifically focusing on CC products and their imagery.

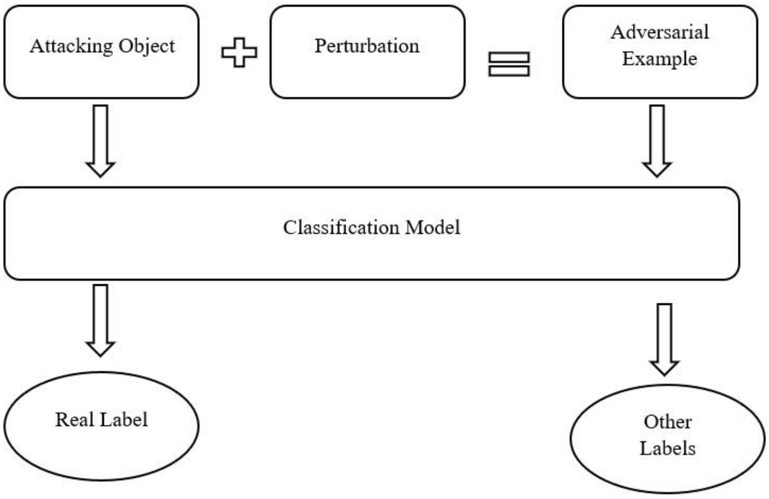

Figure 4. Adversarial Attack Model

Table 1. CIA Triads in the Perspective of Information Security of CC Aesthetics

CIA properties	Explanation
Confidentiality	• Ascertaining that information is available only to proper legitimate users. • The mechanisms to ensure confidentiality aims to protect the images of the CC products from illegitimate access. • It confirms data protection during the transmission phase.
Integrity	• This confirms that the CC aesthetic images should be intact. • The completeness as well as the accuracy of the aesthetics of the image should be ascertained in all phases of processing as well as transmission. • The minor and major changes done to the data must be detected using suitable mechanisms.
Availability	• Confirm that legitimate users have access to assets as and when required.

Recent times have witnessed the usage of AI-based methods to analyze aesthetic elements. These elements do not consider the theory or mathematical elements but design models that learn from the past history of data over which the model is trained. The Machine Learning (ML) and Deep Learning (DL) approaches are found to be superior to other contemporary techniques through their distinct feature extraction property from the training images without relying on handcrafted feature detectors. However, the greatest challenge remains to be assuring the reliability of the defrauding models. These models are not susceptible to detecting minute perturbations. The integrity attacks on CC images impact the model's output which degrades the performance. The aim of creating AdI for CC elements is that adversary examples have a small amount of disturbances or noise that will play the role of testing examples for the models [26]. These examples tap the feature learning of the defrauding DL model and do not completely alter the model.

Exploring the resilience of DL-based fraudulent systems against adversarial examples, the literature [27] offers a variety of defense strategies. Among these, adversarial training, gradient masking, and adversary detection [28] stand out as particularly significant, developed through an in-depth analysis of attack methodologies. Integrating these defense tactics with DL models to safeguard against attacks on integrity can lead to increased computational demands. This highlights the need for an effective defense approach to protect the integrity of aesthetic and artistic creations, an area that continues to be a subject of ongoing research.

This study introduces an innovative Siamese detector, grounded in CNN technology, aimed at thwarting integrity attacks on CC works through image analysis. The approach involves processing images to form a test set. The model then assesses the resemblance between distorted and authentic images using the triplet loss function. Subsequently, it distinguishes between adversarial CC images and their genuine counterparts. The primary focus of this research includes:

(1) Elucidating the significance of integrity-based attacks against Computer vision-based defrauding models.

(2) Constructing a Siamese detector for Computer vision-based defrauding models to mitigate the integrity attacks on the CC aesthetics.

(3) Examining the performance of the model using the custom dataset

The objectives of this Work are described as follows:

- To propose a novel CNN-based Siamese detector that uses Triplet Loss and SGCN for detecting and preventing assaults on the integrity of CC aesthetics.
- To train the model using a large-scale dataset such as ImageNet and evaluate its performance using TL and augmentation approaches on a custom dataset of CC images collected from various sources.
- To evaluate the performance of the model in distinguishing genuine CC elements from those generated by adversarial attacks.

2. Related Works

The use of a sparse matrix for input data has been identified as a potent method to counter adversarial attacks [29]. This technique has shown promising results in safeguarding popular DL models from such attacks. There is a noticeable rise in adversarial attacks targeting text data. To address this, a Recurrent Neural Network (RNN) model incorporating backoff strategies for the application of infrequent words has been developed [30]. Additionally, a novel Key-based Diversified Aggregation method has been employed as a defense mechanism against both gray and black-box attacks [31]. This method's randomization policy effectively bypasses backpropagation in gradient updates, thereby reducing the risk of adversarial attacks. Another innovative approach involves using an untrained iterative method combined with context-independent and dependent character-level features to protect text integrity [32]. Furthermore, robust encodings have been utilized to enhance resilience against adversarial text attacks [33], with the encoding function effectively translating textual data into a discrete space to build a more robust system.

A malware titled Deep Armour [34] is proposed to classify adversarial attacks through a voting system. It deploys popular classifiers to show its competency against white-box attacks. An adversarial watermark that processes fake facial image recognition DL models is proposed [35]. A Cross-Model Universal Adversarial Watermark is employed, which gives a superior performance than its peers. A counterattack model is employed for spam detection with an underlying logistic regression approach [36]. The model used in this work transforms the mail into the form of a bag of segments. A multi-instance regression is applied to each bag. Mingyuan Fan et al. proposed a novel Non-Gradient Attack approach to prevent integrity-based adversarial attacks [37]. Another efficient technique to combat adversarial Fast Gradient Sign attack is proposed by Sahay et al., by compressing as well as denoising the data through a multi-layer Denoising Autoencoder [38]. Novel Saak transforms, which is a representative method for images, is found to be very efficient in mitigating adversarial attacks [39].

The notion of injecting an anti-adversary layer in the existing DL models is also an effective way of combating illegitimate attacks [40]. This approach was useful in detecting black-box adversarial attacks. A Defensive GAN was integrated into a generative model to combat adversarial attacks. Revised Naive Bayes is employed to limit the adversarial attacks by adding weights-based spam and ham [41]. A two-phase spell correction approach with detector and corrector methods to limit adversarial attacks is proposed [42]. This is more efficient on Stanford Sentiment Treebank.

3. Methodology

This part of the work describes the defrauding system, along with the simulated adversarial attack with its defence measure.

The work focuses on building a defrauding system with a simulated adversarial attack with its defence measure that effectively detects the improper or noisy usage of CC element, which may disrupt the brand's market value as the originality of the element getting depicted is altered.

3.1 Siamese Detector as Defrauding System

The designed system incorporates a Siamese Convolutional Neural Network (S-CNN) in tandem with the Triplet Loss function, renowned for its effectiveness in one-shot learning applications [43]. This model employs triplet CNNs that share weights to produce Feature Encodings (FE) of images. The S-CNN utilizes a triplet function, akin to the traditional contrastive loss, for feature absorption, subsequently representing these features as embedding vectors. The incorporation of Triplet Loss enhances the model's capability by ensuring a substantial gap between the similarity measures of positive and negative images, a feat not achievable with contrastive loss. Contrastive loss focuses solely on the marginal difference among dissimilar pairs, often resulting in premature convergence to local minima and thus impeding the differentiation between adversarial and original images.

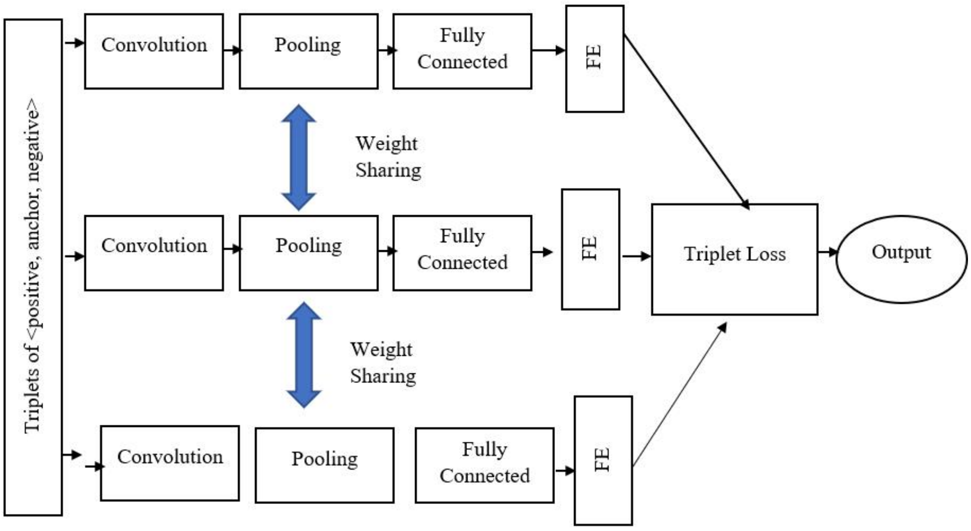

Figure 5. Siamese Network

The feature extraction in convolution layers is governed by Equation 1:

$$f_{i,j}^{(c)} = h\left(\sum_{k=0}^{Cy-1}\sum_{l=0}^{cx-1} w_{k,l}^{c} f_{(i+j,\ k+l)}^{(c-1)} + b^{c} \qquad (1)\right.$$

The factor w_l^c signifies the weight of the neuron at the cth convolutional layer, which is indicated as n(i, j). Commonly, b^c is used as bias. Filter size is specified as c_x x c_y. h depicts the activation function at the given layers. As in any other CNN, a pooling layer will be included after each convolution which down-samples the features to reduce the dimensions. The fully connected layer is responsible for implementing the classifier of the defrauding model. This work uses Graph Convolutional Network. This is a semi-supervised learning method that relies on highly complex graph-structured data structure. The network's convolution layers form a localized first-order approximation capable of scaling the edges. In a S-CNN, the distance between FE for distinct pair will be higher, and vice versa is also true. The triplet loss function learns the FE as triplets in the form of <anchor (I_a), positive (I_p), negative (I_n)> images are:

- Anchor CC element's image that acts as a reference image
- Positive CC element's image, which has the same label as the anchor CC image
- Negative CC element's image whose label is different from that of the anchor as well as a positive image.

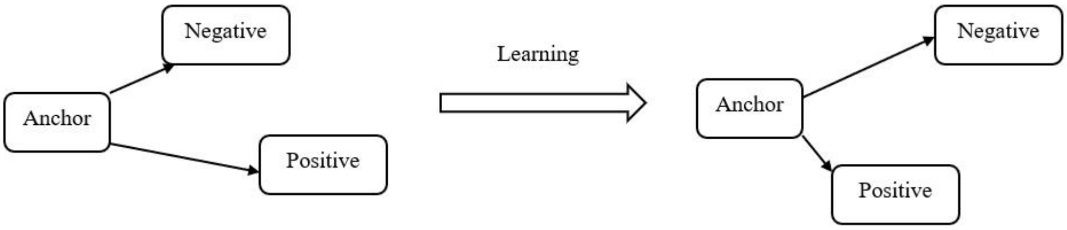

Figure 6. Learning Using Triplet Loss Function.

In this model, the proximity between anchor and positive images is maintained at a smaller scale compared to the distance separating anchor and negative images. The training of parameters, derived from the Feature Encodings (FE), follows the methodology outlined in Equation 2. Within this framework, FE is represented as f(.), and m symbolizes the distance among the clusters created. Additionally, α serves as a normalization constant for the E value.

$$E = \alpha . \sum_{(a,p,n)\epsilon\theta} \max(0, m + \left\|f(I_a) - f(I_p)\right\|_2^2 - \|f(I_a) - f(I_n)\|_2^2) \quad (2)$$

3.2 Adversarial Attack Simulation in the S-CNN

The S-CNN model's vulnerability to adversarial attacks is tested using the enhanced Fast Gradient Sign Method (I-FGSM), a highly effective white-box attack technique that can penetrate the classification layers of the S-CNN network [44]. This approach specifically targets the CC image at its classification layer. Given that digital photos use 8 bits per pixel, the model disregards any information smaller than the constant 1/255. The perturbations added in the image will be a very lower scale which may be ignored by the model while training them. To overcome this issue, the perturbations are increased using the activation by wT φ according to Equation 3:

$$w^T x' = w^T x + w^T \varphi \quad (3)$$

The I-FGSM includes the noise to the images, which is according to the direction of the loss function's gradient and squares it to mitigate the effect of the direction. This work deploys I-FGSM in both targeted and untargeted attacks. The targeted attack alters the input in such a way that the model outputs are very different and predefined, according to Equation 4:

$$ACI= (CCI-\varepsilon \text{ sign } (\Delta_{CCI} J (\theta, CCI, label)))^2 \quad (4)$$

On the other hand, the untargeted attack modifies the input image so that the DL model outputs a different label, which is not already defined according to Equation 5:

$$ACI= (CCI+\varepsilon \text{ sign } (\Delta_{CCI} J (\theta, CCI, label)))^2 \quad (5)$$

In both above equations, Adversarial Chic-China Image (ACI) is the perturbated image, while Clean Chic-China Image (CCI) is the original, clean image. All the images are expressed as width x length x depth. The class label is the output value. The noise level indicators are mentioned as ε and J, and they estimate the cross-entropy loss, which spawns as a function of model parameters, namely loss, CCI and the label. The attack is described in Figure 7.

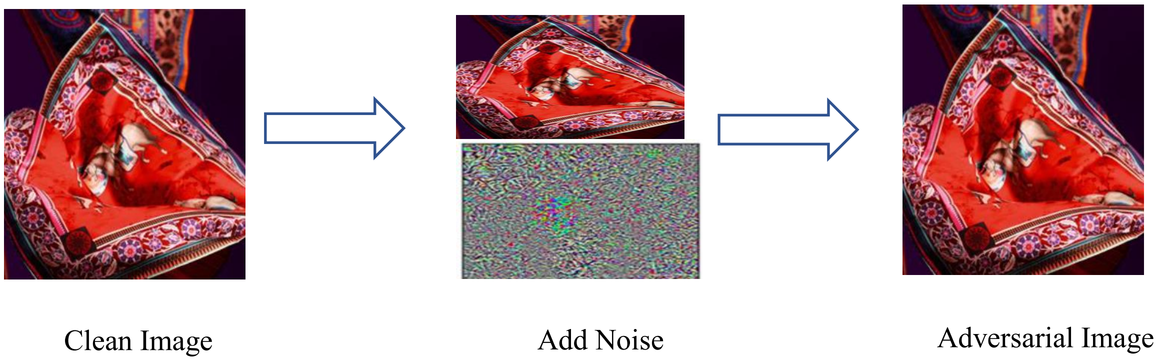

Figure 7. I-FGSM Method of Generating Adversarial Image

3.3 Combating the Adversarial Attack on CC Aesthetic Images using Simplified Graph Convolution Networks

To counteract the injected adversarial attack, the Simplified Graph Convolutional Networks (SGCN) are employed [45]. This method represents an adaptation of CNNs within the framework of graph theory. SGCN achieves protection against adversarial attacks by layering multiple first-order spectral filters, succeeded by a nonlinear activation function. The operational mechanism of the proposed SGCN is depicted in Figure 8.

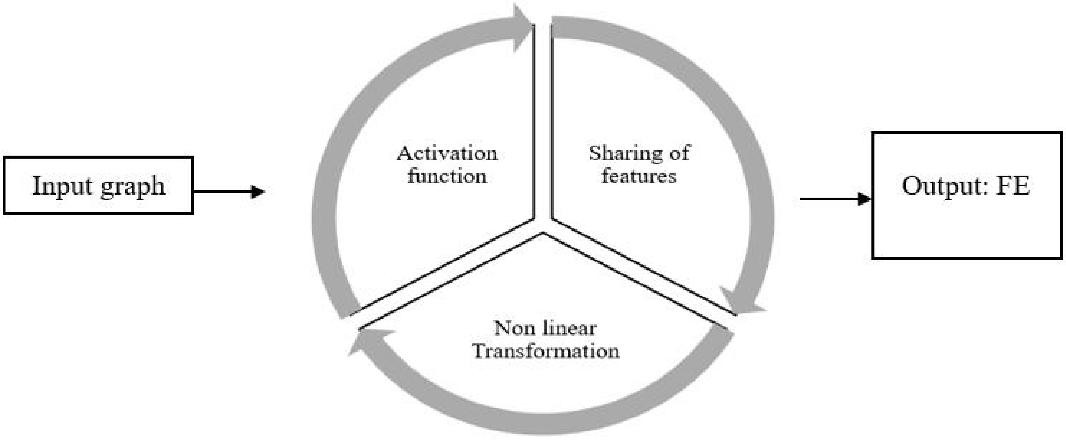

Figure 8. Generation of FE through SGCN

The proposed SGCN quickly extracts the feature f_i in c multiple layers. At any convolution layer, the input is indicated as $A^{c-1,}$ and the output is denoted as A^c. The input features are extracted according to Equation 6:

$$A'^{(0)}= F = [f_1, f_2, \ldots,f_n]^T \tag{6}$$

At the start of each layer, the Feature Propagation process occurs. This involves calculating the average feature (ai) of a node (ni) and its adjacent nodes, as detailed in Equation 7:

$$a_i^k = \frac{1}{d_i + 1} a_a^{k-1} + \sum_{j=1}^{n} \frac{I_{ij}}{\sqrt{(d_i + 1)(d_j + 1)}} a_j^{k-1} \tag{7}$$

This process effectively smooths the Feature Encodings (FE) across the edges while simultaneously spreading analogous predictions to nodes that are locally connected within a specified radius or distance, indicated as d. The weight of each layer, represented by θ^c, is mainly used for linear feature transformation. For the acquisition of non-linear features, the RELU transformation function is utilized, as outlined in Equation (8). The method for obtaining the FE is detailed in Equation 9.

$$Ac \leftarrow ReLU\ (A'^{c}\ \theta^{c}) \qquad (8)$$

$$FE=SA^{c-1}\ \theta^{c} \qquad (9)$$

S is computed in Equation 10. This is the normalized adjacency matrix between the nodes with self-loops to form the graphs.

$$S=D^{-0.5}\ Aj'D^{-0.5} \qquad (10)$$

Aj' is the aggregation of the identity matrix and is estimated by: Aj'=Aj+I. Here Aj is the adjacency matrix of between the edges n_i to $n_{j,}$ and D is degree matrix. This is calculated as D=diag (d_1, d_2, …, d_n). The d value is the row-wise segregation of a_{ij}.

4. Results and Discussion

This section details the experimental analysis of the proposed methodology, which is followed by the results.

4.1 Training the Model

Due to the scarcity and difficulty in acquiring CC images, the model under discussion is trained using the widely recognized ImageNet dataset [46]. The training incorporates 289 and 244 adversarial examples, respectively, created via the FGSM method. Table 2 presents a summary of the training outcomes, with a particular focus on the rates of misclassification within the same collection. The adversarial attack on the SGCN is simulated in a controlled manner. The expectation is that the defrauding systems will exhibit improved misclassification rates, as the Adversarial Images (AdI) should not be categorized as the attacker intends. The training data reveals that the model achieves a 74.01% effectiveness rate, while the S-CNN enhanced with SGCN reaches an effectiveness of 80.11%.

Table 2. Training Results of Adversarial Attack

Name of the Group	Count of Classes	Count of Images	Count of Adversarial Examples created using I-FGSM	Misclassification Rate (S-CNN)	Misclassification Rate (S-CNN combined with SGCN)
Organism	410	9390	9974	73.8%	80.43%
Creature	398	9000	8429	74.3%	81.926%
Domestic Animals	123	2316	3615	73.8%	79.82%
Vertebrates	337	7692	8076	77.73%	80.63%
Mammals	218	4665	5491	71.76%	76.96%
Aquatic Vertebrates	16	336	836	76.45%	81.21%
Birds	59	1956	2064	74.6%	79.24%
Reptiles	36	547	774	73.66%	78.92%
Snake	17	223	343	72.55%	80.08%
Invertebrate	61	1317	1589	72.97%	80.61%
Insect	27	652	561	72.5%	18.36%
Average	***	***	***	74.01%	80.11%

4.2 Testing the Model with CC Images

As the CC images are very rare and have to be collected manually, training the model is done using the popular ImageNet dataset through the Transfer Learning (TL) method. TL applies the knowledge gained to solve a task which is related to another task. The holistic view of TL is shown in described in Figure 9.

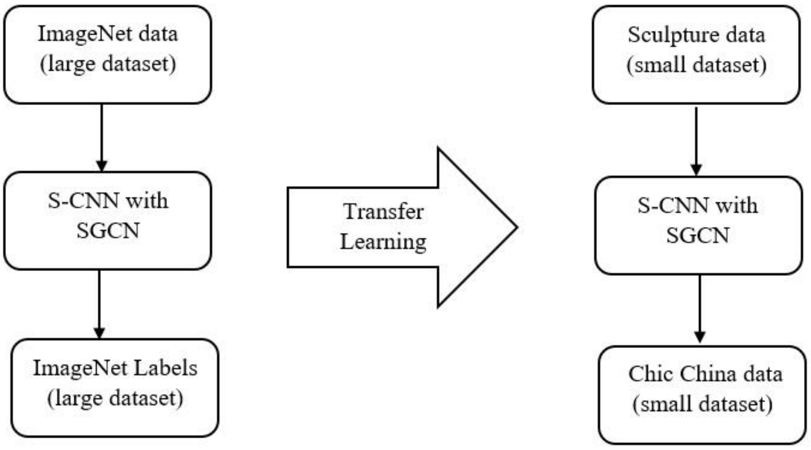

Figure 9. Transfer Learning to Handle Adversarial Attacks

4.3 Training Results of Adversarial Attack

In this study, we showcase the efficacy of our proposed approach in effectively mitigating adversarial attacks on the S-CNN model integrated with SGCN. The efficacy of our approach in identifying Adversarial Chic China Images (ACI) generated through the I-FGSM method is evidenced by the misclassification rates observed across different image classes. The dataset for testing is collected from Google images and other internet sources. Image augmentation is done to increase the randomness and robustness of the data. The images appear raw in their digital format, either partial or full-bodied. The sub-optimal quality images are discarded. The collected images are pre-processed by eliminating undersized and blurry images, as they might affect the prediction accuracy. Also, the augmentation of the original images is done by orienting them by the given angles 300, 600, 900, 1200, 1500, and 1800. The testing images are categorized under six major classes, namely handbags, footwear, sportswear, furnishings, articles and dresses. Table 3 gives the statistics of the images used for testing.

Table 3. Testing Results of Adversarial Attack

Image Class	**Count of Original Images**	**Count of Images after Augmentation**	**Count of AdI**	**Misclassification Rate (S-CNN)**	**Misclassification Rate (S-CNN Combined with SGCN)**
Handbags	24	144	200	78.92%	83.92%
Footwears	30	180	191	74.02%	83.98%
Sportswear	13	78	104	70.92%	80.04%
Dresses	20	120	164	73.56%	79.36%
Furnishings	14	84	96	76.02%	82.63%
Articles	24	144	158	73.82%	80.27%
Average	***	***	***	74.54%	81.7%

4.4 Results of Adversarial Attack Testing

The performance of our proposed method is assessed on a custom dataset comprising aesthetically pleasing images sourced from diverse origins. The model's capability to accurately identify genuine CC elements and differentiate them from fake ones generated via adversarial attacks is evaluated using Transfer Learning (TL) and augmentation methodologies. The results indicate that the prevention of integrity attacks on the S-CNN with SGCN is very effective. The model proposed in the work is nearly 6% more efficient in detecting the AdI of CC elements. These AdI are generated using the FGSM method. As the number of images of CC is small, the model's training is done using a massive ImageNet dataset. The model learns heterogeneous image classes in versatile backgrounds and at various quality levels. As the CC images are relatively low in number, the TL approach comes as a boon that improves the integrity of fake CC elements, thus preserving their aesthetic values. This proposed work is robust and adaptable to combat adversarial attacks on any DL or Computer Vision models. Despite its advantages, the customized dataset used in the testing phase of this work is comparatively small in number, which limits the learning capacity of the model. Nevertheless, the proposed model can be considered the first of its kind in preserving the integrity of CC aesthetics.

The novelty of our research lies in the introduction of a novel approach that integrates Siamese Convolutional Neural Networks (S-CNN) with Triplet Loss and Simplified Graph Convolutional Networks (SGCN) in order to effectively address adversarial attacks on CC aesthetics. Although previous studies may have employed similar methodologies, our research distinguishes itself by focusing on the aesthetics of CC and utilizing a custom dataset. This unique approach enhances the originality of our contribution.

We regret any potential errors in spelling and grammar that may have been present in the manuscript. We will undertake comprehensive proofreading of the entire text in order to enhance its overall quality.

Our Contribution: The contribution of this study lies in formulating a novel methodology designed to effectively tackle the various challenges and concerns associated with the aesthetics of CC. In this study, we present a novel convolutional neural network (CNN)-based Siamese detector that incorporates Triplet Loss and SGCN (Siamese Graph Convolutional Network) to effectively address adversarial attacks targeting connected components (CC) elements. The methodology employed in our study aims to identify and uphold the genuineness of CC aesthetics within the realm of the fashion sector. Although adversarial attacks have been previously explored, our research explicitly addresses the domain of CC aesthetics and their recognition, thereby contributing to the preservation of the cultural authenticity of Chinese designs.

5. Conclusion and Future Works

CC elements have now become a fashionable trend in China, provoking more youth to choose these products. Leading Chinese brands incorporate CC elements into international patterns, which has been seen as a game changer. However, the presence of many forged elements which looks very similar to the original ones is also flooding the market, which may adulterate the original's aesthetic value. Hence, this work proposes the use of the S-CNN defrauding system for detecting the CC aesthetics using the Triplet loss function to aid the learning process. This system is externally attacked with generated AdI, which is created using the I-FGSM method by varying the noise values, accounting for both targeted and non-targeted adversarial attacks that question the integrity of the original elements. Hence, this attack is handled by a novel SGCN, which integrates the prowess of graph functions to learn the FE from the perturbations and to misclassify the adversarial image, which enhances the integrity of the model. The training is done using perturbations generated on the popular ImageNet dataset. The model's efficacy is tested and validated on a custom-made dataset of CC aesthetics by applying TL. The results promise that the proposed model portrays a better misclassification rate, which is a positive sign of any defrauding system. This model could be used to find the presence of real and untarnished CC element which has more aesthetic value in modern days rather than focusing on imparting similar fake elements which may lack preciseness in depicting the original element.

References

[1] P. C. Athukorala, and Z. Wei, "Economic transition and labour market dynamics in China: An interpretative survey of the 'turning point'debate," *Journal of Economic Surveys*, vol. 32, no. 2, pp.420-439, 2018.

[2] S. Lovegren, "Fashionable Food: Seven Decades of Food Fads," *University of Chicago Press*, 2005.

[3] K. Kommonen, "Colours as carriers of myth: The role of the visual in cultural branding," *In Proceedings of AIC08 Conference*, 2008.

[4] Q. Shan Ding, "Chinese products for Chinese people? Consumer ethnocentrism in China," *International Journal of Retail & Distribution Management*, vol. 45, no. 5, pp.550-564, 2017.

[5] J. Paul, "The rise of China: what, when, where, and why?," *The International Trade Journal*, vol. 30, no. 3, pp.207-222, 2016.

[6] P. C. Srivastava, "Leadership styles in Western & Eastern societies and its relation with organizational performance. Pranjana," *The Journal of Management Awareness*, vol. 19, no. 1, pp. 60-76, 2016.

[7] W. Xu, and V. Sirivesmas, "Study on Network Virtual Printing Sculpture Design using Artificial Intelligence," *International Journal of Communication Networks and Information Security*, vol. 15, no. 1, pp.43-51, 2023.

[8] T. Cheng, and A. Marzuki, 2023. "Research on the development of computer digital technology combined with commercial space landscape design in the theory of" design combined with nature," *International Journal of Communication Networks and Information Security*, vol. 15, no. 1, pp.84-94.

[9] T. Ferrero-Regis, and T. Lindgren, "Branding "created in China": The rise of Chinese fashion designers," *Fashion Practice*, vol. 4, no. 1, pp.71-94, 2012.

[10]C. Tsui, "The design theory of contemporary "chinese" fashion," *Design Issues*, vol. 35, no. 3, pp.64-75, 2019.

[11]P. L. P.Rau, E. Huang, M. Mao, Q. Gao, C. Feng, and Y. Zhang, "Exploring interactive style and user experience design for social web of things of Chinese users: A case study in Beijing," *International Journal of Human-Computer Studies*, vol. 80, pp.24-35, 2015.

[12]Z. Han, D. Xu, and R. Zheng, "China-chic: From Chinese Elements to International Trend," *8th International Conference on Humanities and Social Science Research (ICHSSR 2022)* (pp. 2499-2504). Atlantis Press, 2022.

[13]L. L. Mao, and J. Zhang, "Branding through sponsorship-linked marketing: A case of Chinese sports apparel and equipment brand 'Li Ning'," *In Digital marketing and consumer engagement: Concepts, methodologies, tools, and applications* (pp. 191-214). 2018. IGI Global.

[14]L. Zhang, M. Li, L. Zhang, X. Liu, Z. Tang, and Y. Wang, "MasterSu: The sustainable development of Su embroidery based on digital technology," *Sustainability*, vol. 14, no. 12, p.7094, 2022.

[15]Y. Dai, X. Song, and Z. Zhang, "Why Have Many 'Time-Honored Brands' Begun to Take the China-Chic?," *In 2021 International Conference on Public Relations and Social Sciences (ICPRSS 2021)* (pp. 49-53). 2021. Atlantis Press.

[16]X. Luo, K. Wang, X. Zhang, L. Deng, Y. Luo, and C. Luo, "Rapid Light-curve Changes and Probable Flip-flop Activity of the W UMa-type Binary V410 Aur," *The Astronomical Journal*, vol. 154, no. 3, pp. 99, 2017.

[17]Z. Han, D. Xu, and R. Zheng, "China-chic: From Chinese Elements to International Trend," *In 2022 8th International Conference on Humanities and Social Science Research (ICHSSR 2022)* (pp. 2499-2504). 2022. Atlantis Press.

[18]D. Tamburini, C. R. Cartwright, M. Pullan, and H. Vickers, "An investigation of the dye palette in Chinese silk embroidery from Dunhuang (Tang dynasty)," *Archaeological and Anthropological Sciences*, vol. 11, pp.1221-1239, 2019.

[19]Y. Wang, A. Hong, X. Li, and J. Gao, "Marketing innovations during a global crisis: A study of China firms' response to COVID-19," *Journal of business research*, vol. 116, pp.214-220, 2020.

[20]F. Li, S. Frederick, and G. Gereffi, "E-commerce and industrial upgrading in the Chinese apparel value chain," *Journal of Contemporary Asia*, vol. 49, no. 1, pp.24-53, 2019.

[21]D. C. Gladney, "Representing nationality in China: Refiguring majority/minority identities," *The Journal of Asian Studies*, vol. 53, no. 1, pp.92-123, 1994.

[22]V. S. Chand, and C. Fei, "Self-brand connection and intention to purchase a counterfeit luxury brand in emerging economies," *Journal of Consumer Behaviour*, vol. 20, no. 2, pp. 399-411, 2021.

[23]S. Sharanya, R. E. V. A. T. H. I.Venkataraman, and G. Murali, "Estimation of remaining useful life of bearings using reduced affinity propagated clustering," *Journal of Engineering Science and Technology*, vol. 16, no. 5, pp.3737-3756, 2021.

[24]E. Sasikala, R. Radha, S. Sharanya, and M. Gayathri, "Artificial neural networks with vertical handoff prediction based on user behaviour," *Pakistan Journal of Biotechnology*, vol. 15, no. 1, pp.89-93, 2018.

[25]H. Xu, Y. Ma, H. C. Liu, D. Deb, H. Liu, J. L. Tang, and A. K. Jain, “Adversarial attacks and defenses in images, graphs and text: A review,” *International Journal of Automation and Computing*, vol. 17, pp.151-178, 2020.

[26]E. Soares, “Radnn: Robust to imperceptible adversarial attacks deep neural network,” 2021.

[27]F. Liao, M. Liang, Y. Dong, T. Pang, X. Hu, and J. Zhu, “Defense against adversarial attacks using high-level representation guided denoiser,” *In Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1778-1787), 2018.

[28]S. G. Finlayson, J. D. Bowers, J.Ito, J.L.Zittrain, A.L.Beam, and I.S.Kohane, “Adversarial attacks on medical machine learning,” *Science*, vol. 363, no. 6433, pp.1287-1289, 2019.

[29]S. Gopalakrishnan, Z. Marzi, U. Madhow, and R. Pedarsani, “Combating adversarial attacks using sparse representations,” *arXiv preprint arXiv:1803.03880*, 2018.

[30]D. Pruthi, B. Dhingra, and Z. C. Lipton, “Combating adversarial misspellings with robust word recognition,” *arXiv preprint arXiv:1905.11268*, 2019.

[31]O. Taran, S. Rezaeifar, T. Holotyak, and S. Voloshynovskiy, “Machine learning through cryptographic glasses: combating adversarial attacks by key-based diversified aggregation,” *EURASIP journal on information security*, vol. 2020, no. 1, pp.1-18, 2020.

[32]Y. Keller, J. Mackensen, and S. Eger, “BERT-defense: A probabilistic model based on BERT to combat cognitively inspired orthographic adversarial attacks,” *arXiv preprint arXiv:2106.01452*, 2021.

[33]E. Jones, R. Jia, A. Raghunathan, and P. Liang, “Robust encodings: A framework for combating adversarial typos,” *arXiv preprint arXiv:2005.01229*, 2020.

[34]Y. Ji, B. Bowman, and H. H. Huang, “Securing malware cognitive systems against adversarial attacks,” In *2019 IEEE international conference on cognitive computing (ICCC)* (pp. 1-9). 2019.

[35]H. Huang, Y. Wang, Z. Chen, Y. Zhang, Y. Li, Z. Tang, W. Chu, J. Chen, W. Lin, and K. K. Ma, “Cmua-watermark: A cross-model universal adversarial watermark for combating deepfakes,” In *Proceedings of the AAAI Conference on Artificial Intelligence* ,vol. 36, no. 1, pp. 989-997, 2022.

[36]Z. Jorgensen, Y. Zhou, and M. Inge, “A Multiple Instance Learning Strategy for Combating Good Word Attacks on Spam Filters,” *Journal of Machine Learning Research*, vol. 9, no. 6, 2008.

[37]Fan, M., Liu, Y., Chen, C., Yu, S., Guo, W., & Liu, X. ,“Combating false sense of security: Breaking the defense of adversarial training via non-gradient adversarial attack,” *ICASSP IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2022, pp. 3293-3297.

[38]R. Sahay, R. Mahfuz, and A. E. Gamal, “A computationally efficient method for defending adversarial deep learning attacks,” *arXiv preprint arXiv:1906.05599*, 2019.

[39]M. Alfarra, J. C.Pérez, A. Thabet, A. Bibi, P. H. Torr, and B. Ghanem, “Combating adversaries with anti-adversaries,” *In Proceedings of the AAAI Conference on Artificial Intelligence* , vol. 36, no. 6, pp. 5992-6000, 2022,

[40]P. Samangouei, M. Kabkab, and R. Chellappa,,”Defense-gan: Protecting classifiers against adversarial attacks using generative models,” *arXiv preprint arXiv:1805.06605,* 2018.

[41]J. Peng, and P. P. Chan, “Revised Naive Bayes classifier for combating the focus attack in spam filtering,” *In 2013 International Conference on Machine Learning and Cybernetics* (vol. 2, pp. 610-614). 2013, IEEE.

[42]Z. Liu, F. Wang, Z. Lin, L. Wang, and Z. Yin, “De-co: A two-step spelling correction model for combating adversarial typos,” *In 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* (pp. 554-561). 2020, IEEE.

[43]D. Shi, M. Orouskhani, and Y. Orouskhani, “A conditional Triplet loss for few-shot learning and its application to image co-segmentation,” *Neural Networks*, vol. 137, pp.54-62, 2021.

[44]X. Yuan, P. He, Q. Zhu, and X. Li, “Adversarial examples: Attacks and defenses for deep learning,” *IEEE transactions on neural networks and learning systems*, vol. 30, no. 9, pp.2805-2824, 2019.

[45]A. A. Yusuf, F. Chong, and M. Xianling, “An analysis of graph convolutional networks and recent datasets for visual question answering,” *Artificial Intelligence Review*, vol. 55, no. 8, pp.6277-6300, 2022.

[46]J. Deng, W. Dong, R. Socher, L. J. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” *In 2009 IEEE conference on computer vision and pattern recognition* (pp. 248-255). 2009. IEEE.